**KİŞİSEL VERİ SAKLAMA, İMHA VE ANONİMLEŞTİRME POLİTİKASI**

# KAPSAM

* 1. İşbu Kişisel Veri Saklama, İmha ve Anonimleştirme Politikası (“**Politika**”); **Grow Fide Üretim ve Ticaret A.Ş.**’nin (“**Şirket**”) Kişisel Verileri işlediği herhangi bir sürece dâhil olan tüm departmanlarını, çalışanlarını ve 3. partileri kapsamaktadır.
  2. İşbu Politika; Şirket’in Kişisel Veriler üzerinde uygulayacağı tüm İmha faaliyetlerini kapsayacak olup, her türlü İmha gereksinimi sonucunda uygulanacaktır.
  3. İşbu Politika Kişisel Veri olmayan veriler hakkında uygulanmayacaktır.
  4. Konuyla alakalı yeni mevzuatın belirlenmesi veya ilgili mevzuatın güncellenmesi durumunda, Şirket Politika’yı ilgili mevzuata uyumlu olacak şekilde güncelleyerek mevzuat gerekliliklerine uyacaktır.
  5. İşbu Politika’nın Şirket tarafından uygulanmasında hukuki bir engel olduğuna kanaat getirildiği durumlarda, Şirket uygulayacağı adımları gerek görülmesi durumunda yeniden belirleyebilecektir.

# TANIMLAR

|  |  |  |
| --- | --- | --- |
| **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. | |
| **Anonim Hale**  **Getirme veya**  **Anonimleştirme** | Kişisel Verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. | |
| **Anonim Hale Getirilmiş Veri** | Başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmiş veriyi ifade eder. | |
| **İmha** | Kişisel silinmesi, yok edilmesi ve anonim hale getirilmesini ifade eder. | |
| **İlgili Kullanıcı** | Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere Veri Sorumlusu organizasyonu içerisinde veya Veri Sorumlusundan aldığı yetki ve talimat doğrultusunda Kişisel Verileri işleyen kişileri ifade eder. | |
| **Kanun** | 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nu 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 (işbu Politika kapsamında “Kişisel Veri” ifadesi uygun olduğu ölçüde aşağıda tanımlanan Özel Nitelikli Kişisel Veriler’i de kapsayacaktır). |
| **Kişisel Veri İşleme** | | Kişisel Verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veri üzerinde gerçekleştirilen her türlü işlemi ifade eder. |
| **KVK Yetkilisi** | | İşbu Politikanın ve Politikaya bağlı olarak uygulanacak KVK Prosedürlerinin yerine getirilmesinden sorumlu KVK Yetkilisi’ni ifade eder (Veri Sorumlusu Temsilcisi ile aynı veya farklı bir kişi belirlenebilir). |
| **Kurul** | | Kişisel Verileri Koruma Kurulu’nu ifade eder. |
| **Kurum** | | Kişisel Verileri Koruma Kurumu’nu ifade eder. |
| **KVK Düzenlemeleri** | | 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Kişisel Verilerin korunmasına yönelik ilgili diğer mevzuatı, düzenleyici ve denetleyici otoriteler, mahkemeler ve diğer resmi makamlar tarafından verilen, bağlayıcı kararları, ilke kararlarını, hükümleri, talimatları ile verilerin korunmasına yönelik uygulanabilir uluslararası anlaşmaları ve diğer her türlü mevzuatı ifade eder. |
| **KVK Prosedürleri** | | Şirketin, çalışanların, KVK Yetkilisinin ve Veri Sorumlusu Temsilcisinin işbu Politika kapsamında uyması gereken yükümlülükleri belirleyen prosedürleri ifade eder. |
| **Politika** | | Şirket’in, Kişisel Verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile Silme, Yok Etme ve Anonim Hale Getirme işlemi için dayanak yaptığı Kişisel Veri Saklama, İmha ve Anonimleştirme Politikası’ni ifade eder. |
| **Sicil** | | Başkanlık tarafından tutulan Veri Sorumluları Sicili’ni ifade eder. |
| **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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri ifade eder. |
| **Silme veya Silinme** | | Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini ifade eder. |
| **Veri Envanteri** | | Şirketin iş süreçlerine bağlı olarak gerçekleştirmekte olduğu Kişisel Veri İşleme faaliyetlerini; Kişisel Veri İşleme amaçları, veri kategorisi, Kişisel Verilerin aktarıldığı Alıcı Grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve Kişisel Verilerin İşlendiği amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen Kişisel Verileri ve veri güvenliğine ilişkin alınan tedbirleri  açıklayarak detaylandırdıkları envanteri ifade eder |
| **Veri Kayıt Sistemi** | | Kişisel Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder. |
| **Veri Öznesi** | | Kişisel Verileri Şirket tarafından veya Şirket adına işleme sokulan tüm gerçek kişileri ifade etmektedir. |
| **Veri Sorumlusu** | | Kişisel Verileri işleme amaçları ve işleme yollarını belirterek işleyen, Veri Kayıt Sisteminin kurulması ve yönetilmesi sorumluluğu bulunan gerçek veya tüzel kişiyi ifade etmektedir. |
| **Veri Sorumlusu Temsilcisi** | | KVK Yetkilisi içerisinden seçilen ve Şirketin Kurum ile olan ilişkilerini yürüten ve yönetim kurulu kararı ile atanan çalışanı ifade etmektedir. |
| **Yönetmelik** | | Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik’i ifade etmektedir. |
| **Yok Etme** | | Kişisel Verilerin, hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder. |

Kişisel Verilerin Korunması ve Gizliliği Politikası içerisinde bulunan tanımlar işbu Politika için de geçerlidir.

# AMAÇ VE KAPSAM

* 1. İşbu Politika, Kanunun 7.maddesi uyarınca oluşturulan Yönetmelik içerisinde yer alan Kişisel Verilerin Silinmesinden, Yok Edilmesinden veya Anonim Hale Getirilmesinden sorumlu olan gerçek veya tüzel kişiler hakkında uygulanacak ve Şirket ile Şirket’in sözleşmesel olarak sorumlu kıldığı üçüncü kişiler tarafından uyulması gereken esasları belirleyecektir.
  2. Yönetmelik uyarınca Şirket, Sicile kayıt yükümlülüğü olan bir Veri Sorumlusu olarak, Kişisel Verileri, uhdesinde bulunan Veri Envanteri’ne uygun bir şekilde saklamak ve gerektiğinde Silmek, Yok Etmek ya da Anonim Hale Getirmek için bir Politika hazırlamak ve bu Politikaya uygun hareket etmek ile yükümlüdür. Bu kapsamda Şirket, sayılan yükümlülükleri yerine getirmek amacıyla işbu Politika’yı hazırlamıştır.
  3. Kişisel Verilerin saklanması ve imhasında aşağıdaki ilkeler geçerli olacaktır:
     1. Kanunun 4. maddesindeki genel ilkelere ve Yönetmelik’in 7. maddesindeki ilkelere uyulacaktır.
     2. Şirket, işbu Politikayı hazırlamış olmanın tek başına Kişisel Verilerin Yönetmelik, Kanun ve KVK Düzenlemelerine uygun olarak Silindiği, Yok Edildiği veya Anonim Hale Getirildiği anlamına gelmeyeceğini kabul etmektedir.
     3. Şirket, Kişisel Verileri saklarken yahut Silerken, Yok Ederken veya Anonim Hale Getirirken, Kanunun 12. maddesinde yer alan güvenlik tedbirlerine, KVK Düzenlemelerine ve Politikaya uygun hareket edeceğini kabul, beyan ve taahhüt eder.
     4. Şirket, bünyesinde bulundurduğu Kişisel Verilerin amacı tamamen veya kısmen otomatik olan ya da herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi sırasında İşbu Politika’ya ve Politika’ya bağlı olarak uygulanacak araç, program ve süreçlere uygunluk sağlayacağını taahhüt eder.

# KAYIT ORTAMLARI

* 1. Şirket, işbu Politika ile Kişisel Veri içeren ve aşağıda sayılmış olan ortamlar ve bunlara ek olarak ortaya çıkabilecek diğer ortamlardaki Kişisel Verileri Politikanın kapsamına dahil etmeyi kabul eder:
     1. Şirket adına kullanılan bilgisayarlar/sunucular,
     2. Ağ cihazları,
     3. Ağ üzerinde veri saklanması için kullanılan paylaşımlı/paylaşımsız disk sürücüleri
     4. Bulut sistemleri,
     5. Mobil telefonlar ve içerisindeki tüm saklama alanları,
     6. Kağıt,
     7. Mikrofiş,
     8. Yazıcı, Parmak izi okuyucu gibi çevre birimler,
     9. Manyetik bantlar,
     10. Optik diskler,
     11. Flash hafızalar.

# KİŞİSEL VERİLERİN SAKLANMASINI VE İMHASINI GEREKTİREN DURUMLAR

Aşağıda belirtilen kapsamda bir ihlal olması durumunda potansiyel güvenlik ihlal durumu kabul edilerek Şirket tarafından önlem alınacaktır. Şirket, Kişisel Verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır.

* 1. **Kişisel Verilerin Saklanmasını Gerektiren Durumlar**

Şirket; (i) kanunlarda açıkça öngörülmesi, (ii) fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, (iii) bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, (iv) hukuki yükümlülüğün yerine getirebilmesi için zorunlu olması (v) bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, (vi) Veri Öznesi’nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, Veri Sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerindenKişisel Verileri mevzuata uygun olarak saklamakla yükümlüdür. Şirket ayrıca; (i) Açık Rıza alınması, (ii) Kanun’un 5(2) ve 6(3) maddelerinde yer verilen istisnaların bulunması durumunda Kişisel Verileri saklama hakkını haizdir.

* 1. **Kişisel Verilerin İmhasını Gerektiren Durumlar**
     1. **Kanun’a Aykırılık**

Şirket, Kişisel Verileri Kanun’da belirtildiği şekle aykırı olarak işlemeyeceğini taahhüt eder.

Şirket, Kanun’un 5 ve 6. maddelerindeki Kişisel Verilerin ve Özel Nitelikli Kişisel Verilerin işlenmesi şartlarındaki istisnalar mevcut olmadığı sürece;

* + - 1. Kanun’da belirtilen istisnalar dışında Açık Rızasını almadığı kişilerin Kişisel Verilerini saklamaz.
      2. Şirket, Özel Nitelikli Kişisel Verileri sakladığı durumlarda, verileri KVK Düzenlemelerine bağlı kalarak KVK Yetkilisi’nin bilgisi dâhilinde işler. Bu kapsamda Kanun’un 6(4) maddesi kapsamında Kurul tarafından belirlenmiş ya da belirlenecek tedbirleri alır.
    1. **Veri İşleme Şartlarının Ortadan Kalkması**

Şirket, veri işlenme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu tüm çalışanları ile paylaşır.

Çalışanlar, veri işlenme şartlarının tamamının ortadan kalktığı durumlarda veri işlemeye devam edemez. Şirket ilgili bilgi işlem çalışan veya hizmet verenleri, şartların ortadan kalktığı Kişisel Verileri işbu Politika’ya uygun bir şekilde Silmek, Yok Etmek ya da Anonim Hale Getirmekle yükümlüdür. Şirket aşağıda listelenen ve Yönetmelik içinde de belirtilen ilgili durumlarda veri işlenme şartlarının ortadan kalktığını kabul eder:

* + - 1. Kişisel Verileri işlemeye esas teşkil eden KVK Düzenlemelerinin değiştirilmesi veya yürürlükten kaldırılması,
      2. Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçersiz olması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
      3. Kişisel Verilerin işlenmesini gerektiren amacın ortadan kalkması,
      4. Kişisel Verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,
      5. Kişisel Verileri işlemenin sadece Açık Rıza şartına istinaden gerçekleştiği hallerde, Veri Öznesinin rızasını geri alması,
      6. Veri Öznesinin, Kanunun 11.maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde Kişisel Verileri işleme faaliyetine ilişkin usule uygun başvuru yapması,
      7. Veri Sorumlusunun, Veri Öznesi tarafından Kişisel Verilerinin Silinmesi veya Yok Edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,
      8. Kişisel Verilerin saklanmasını gerektiren azami süre geçmiş olmasına rağmen, Kişisel Verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

1. **KİŞİSEL VERİLERİN SAKLANMASI, İŞLENMESİ VE İMHASI İÇİN ALINAN TEDBİRLER**

Şirket, Kişisel Verilerin hukuka uygun şekilde saklanması, işlenmesi ve erişimini sağlamak için korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetlerine göre teknik ve idari tedbirler almaktadır.

* 1. **Teknik Tedbirler**

Şirket tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca teknik tedbirler aşağıda sıralanmaktadır:

* + 1. Teknolojideki gelişmelere uygun teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmekte ve yenilenmektedir.
    2. İş birim bazlı belirlenen hukuksal uyum gerekliliklerine uygun olarak yetki matrisi oluşturulmuş, kişisel hesap yönetimi sistemi kurulmuş ve şifreleme sistemleri aktive edilmiştir.
    3. Bu kapsamda virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılım ve donanımlar kurulmakta, log kayıtları tutulmakta, düzenli yedeklemeler yapılmaktadır.
    4. Ağ güvenliğini sağlamak için gerekli yazılım ve donanım kurulmakta, yetki kontrolleri ve sızma testleri 6 aylık aralıklarla gerçekleştirilmektedir. Bu kapsamda güvenlik duvarları ve saldırı tespit ve önleme sistemleri kullanılmaktadır.
    5. Alınan teknik önlemler periyodik olarak iç denetim mekanizması gereği KVK Yetkilisi’ye raporlanmakta, risk teşkil eden hususlar yeniden değerlendirilerek gerekli teknolojik çözüm üretilmektedir.
    6. Açık Rıza alınmayan ve kanuni istisnalar arasına girmeyen veriler maskelenerek kullanılmaktadır
    7. Teknik konularda bilgili personel istihdam edilmekte veya bu amaçla dış kaynaklardan hizmet ve destek alınmaktadır.
  1. **İdari Tedbirler**

Şirket tarafından Kişisel Verilerin hukuka aykırı saklanması, işlenmesi ve erişimini engellemek için alınan başlıca idari tedbirler aşağıda sıralanmaktadır:

* + 1. Şirket çalışanlarına Kişisel Verileri Koruma mevzuatı kapsamında bilgilendirmiş ve bu konuda gerekli eğitimlerden geçirmiştir. Çalışanlar ile, öğrendikleri Kişisel Verileri KVK Düzenlemelerine aykırı olarak başkasına açıklayamayacağı, işleme amacı dışında kullanamayacağı ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda gizlilik sözleşmesi imzalanarak Kişisel Verilerin korunması adına gerekli taahhütler alınmıştır. Bu kapsamda çalışan iş sözleşmeleri ve disiplin yönetmeliklere Kanun’a uygun hükümler eklenmiştir. Şirket içi organizasyonlarında, bu taahhütlere ve sair gizlilik yükümlülüklerine uyulmaması durumunda işletilecek disiplin süreçlerini hazırlamıştır.
    2. Şirket çalışanlarını 6 aylık aralıklarla bilgilendirmeye devam edeceğini ve bilgilerini güncel tutacağını taahhüt etmektedir.
    3. Sicile bildirim yapılabilmesi için gerekli hazırlıklarını tamamlamıştır.
    4. İş birimi bazlı hukuksal uyum gerekliliklerine uygun olarak Şirket içinde Kişisel Verilere erişim ve yetkilendirme süreçleri tasarlanmış ve uygulanmaktadır.
    5. Şirket tarafından Kişisel Verilerin hukuka uygun olarak aktarıldığı kişiler ile akdedilen sözleşmelere; Kişisel Verilerin aktarıldığı kişilerin, Kişisel Verilerin korunması amacıyla gerekli güvenlik tedbirlerini alacağına ve kendi kuruluşlarında bu tedbirlere uyulmasını sağlayacağına ilişkin hükümler eklenmektedir.
    6. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında işbu Politika kapsamında gerekli düzenlemeleri yapmıştır
    7. Veri Envanteri hazırlanmış ve Kişisel Verilerin işlenmesi, muhafazası ve aktarılmasına ilişkin sözleşmelerde gerekli hükümlere yer vermiş,
    8. Kurum İçi Periyodik ve/veya Rastgele Denetimler için gerekli hazırlıklar yapılmıştır. Risk Analizleri gerçekleştirilerek gerekli önlemler alınmıştır.
    9. İhlal durumunda kurumsal iletişim prosedürleri ve bilgilendirme süreçleri işbu Politika’da belirleniştir.
  1. **Kişisel Verilerin Korunması Konusunda Alınan Tedbirlerin Denetimi**

Şirket, KVK Kanunu’nun 12. maddesine uygun olarak, kendi bünyesinde oluşturduğu KVK Yetkilisi aracılığı ile gerekli denetimleri yapmakta veya yaptırmaktadır. Bu denetim sonuçları Şirketin iç işleyişi kapsamında konu ile ilgili bölüme raporlanmakta ve alınan tedbirlerin iyileştirilmesi için gerekli faaliyetler yürütülmektedir.

1. **KİŞİSEL VERİLERİN YETKİSİZ BİR ŞEKİLDE İFŞASI**

Şirket Kanun’da, KVK Düzenlemelerinde ve işbu Politikada yer verilen Kişisel Veri güvenliği yükümlülüklerinin ihlali durumlarında izlenecek prosedürü işbu Politika kapsamında düzenlemiştir.

* 1. **Şirket Bünyesinde Gerçekleşen İhlaller**

Bir Şirket çalışanı herhangi bir ihlal tespit etmesi veya olası bir ihlalle karşılaşması durumunda ilgili yönetici ve KVK Yetkilisini durumdan derhal haberdar eder, ihlalin nasıl farkına varıldığı ve nereden kaynaklandığı konusunda bilgilendirir. Yönetici ve KVK Yetkilisi ihlali devam ediyorsa durdurmak ve sona ermişse boyutunu tespit etmek adına ilk önlemleri alır ve Yönetim Kurulunu durumdan haberdar eder. Yetkili, ihlal karşısında önlem alması için bilgi işlem departmanından destek alır ve hukuk departmanı ile iletişime geçer ve incelemeler neticesinde sonuçlarını raporlayarak Yönetim Kurulu ve Kurum ile paylaşır.

* 1. **Üçüncü Kişiler Bünyesinde Gerçekleşen İhlaller**

KVK Yetkilisi Başkanı, Şirket’in çalıştığı üçüncü bir kişinin herhangi bir ihlal tespit etmesi veya olası bir ihlalle karşılaşması durumunda, haber verilmesini takip eden on iki saat içerisinde hukuk departmanı ve gerekiyorsa IT departmanı ile iletişime geçer. Başkan, KVK Yetkilisi’yi haber verilmesini takip eden 24 saat içerisinde toplar; ihlalin boyutu, kapsamı ve sonuçları hakkında karşı taraftan elde ettiği bilgileri raporlayarak Yönetim Kurulu ve Kurum ile paylaşır.

# KİŞİSEL VERİLERİN İMHASI

Kişisel Verilerin İmhası, verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi şeklinde üç farklı şekilde sağlanabilir. İmha işlemindeki amaç, kalan veriler ile gerçek kişiye ulaşabilmenin mümkün olmamasıdır. Şirket, Kişisel Verilerin hukuka uygun olarak Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır.

* 1. **Kişisel Verilerin Silinmesi**

Tamamen veya kısmen otomatik yollarla işlenen Kişisel Verilerin silinmesi; söz konusu Kişisel Verilerin İlgili Kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Veri Sorumlusu, ilgili politika ve prosedürlerinde Kişisel Verilerin Silinmiş sayılması için Yönetmelik madde 7(3)’te belirtilen koşulların nasıl sağlandığını açıklar. Herhangi bir Veri Kayıt Sisteminin parçasını teşkil eden ve otomatik olmayan yollarla işlenen Kişisel Verilerin silinmesi; tarama yoluyla veya sayısallaştırılmadan elektronik ortama aktarılan kağıt halindeki gerekli olmayan Kişisel Verilerin Anonim Hale Getirilmesi yoluyla gerçekleştirilme işlemi, Şirket’in verileri tamamen veya otomatik yollarla işlediği durumlarda yapılır ve Şirket, Kişisel Verileri sildiği durumlarda, verileri hiçbir şekilde erişilemez veya tekrar kullanılamaz hale getirir. Şirket, bu işlemi yaparken verilerin hiçbir kullanıcı tarafından erişilemez veya tekrar kullanılamaz olduğunu garanti eder. Bu garanti, Şirket’in sorumluluğu altındadır. Belirtilen Silme yöntemleri, Yönetmelik’e bağlı olup ilgili durumlarda güncellenmesi Şirket’in sorumluluğundadır.

* 1. **Kişisel Verilerin Yok Edilmesi**

Yok Etme işlemi, Şirket’in verileri fiziksel kayıt ortamlarında işlediği durumlarda yapılacaktır ve Şirket bu verileri erişilemeyecek, tekrar kullanılamayacak ve tekrar geri getirilmesi mümkün olmayacak hale getirmekle yükümlüdür.

Yok Etme işlemleri sırasında Şirket çalışanları ve ilgili departmanlar KVK Yetkilisi’ne yok edilecek ilgili verileri bildirmekle yükümlüdür, sonrasında ise Şirket gerekli her türlü teknik ve idari tedbiri alacaktır.

* 1. **Kişisel Verilerin Anonimleştirilmesi**

Anonim Hale Getirme işlemi, Şirket’in Kişisel Verileri tamamen veya otomatik yollarla işlediği durumlarda, bu verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel Verilerin Anonim Hale Getirilmesi Şirket içerisinde veri sahibi iş biriminin görevidir. Veri sahibi iş birimi, verilerin anonim hale getirilmesi için denetimi kendisi tarafından yapılmak kaydıyla Şirket’in farklı departmanlarından destek alabilir.

Kişisel Verilerin Anonim Hale Getirilmesi sırasında Şirket, işbu Politika kapsamında belirtilen yöntemleri kullanılabilir. Uygulanacak yöntemin doğruluğundan emin olunamadığı durumlarda KVK Yetkilisi’ne danışılmalıdır.

# KİŞİSEL VERİLERİN İMHA YÖNTEMLERİ VE SÜRECİ

Kişisel Verilerin İmhası için Şirket, imha sırasında kullanılabilecek tüm yöntemleri işbu Politika’da tanımlar. Veri sahibi iş birimi, İşbu Politika içerisindeki uygun yöntemi uygun duruma göre belirleyerek uygulamakla yükümlüdür.

Şirket, Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re’sen siler, yok eder veya anonim hale getirir.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

**3.2.1.1 Silme Yöntem​leri**

|  |  |  |
| --- | --- | --- |
| Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri | | |
| Karartma | : | Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemez hale getirilmesi şeklinde yapılır. |
| Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri | | |
| Yazılımdan güvenli olarak silme | : | Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz. |

**3.2.1.2 Yok Etme Yöntemleri**

|  |  |  |
| --- | --- | --- |
| Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri | | |
| Fiziksel yok etme | : | Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir. |
| Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri | | |
| Fiziksel yok etme | : | Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. |
| De-manyetize etme (degauss) | : | Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir. |
| Üzerine yazma | : | Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1’lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir. |
| Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri | | |
| Yazılımdan güvenli olarak silme | : | Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz. |

**3.2.1.3. Anonimleştirme Yöntemleri**

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

|  |  |  |
| --- | --- | --- |
| Değişkenleri çıkarma | : | İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da bir kaçının çıkarılmasıdır.  Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir. |
| Bölgesel gizleme | : | Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir. |
| Genelleştirme | : | Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir. |
| Alt ve üst sınır kodlama / Global kodlama | : | Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir.  Aynı kategori içinde kalan değerler birleştirilir. |
| Mikro birleştirilme | : | 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. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olacağından, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır. |
| Veri karma ve bozma | : | Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır. |

Şirket, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. Şirket, bu anonimleştirme yöntemlerini kullanırken K-Anonimlik [UN2] (K-Anonymity), L-Çeşitlilik (L-Diversity) [UN3] ve T-Yakınlık [UN4] (T-Closeness) istatistik yöntemlerini kullanabilir

# SAKLAMA VE İMHA SÜRELERİ

* 1. **Periyodik İmha ve Yasal Saklama Süreleri**

Yasal saklama ve İmha sürelerini dolduran fiziksel ve dijital veriler, periyodik olarak İmha edilir. Şirket, Kişisel Verileri Silme, Yok Etme veya Anonim Hale Getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk Periyodik İmha işleminde, Kişisel Verileri Siler, Yok Eder veya Anonim Hale Getirir. Periyodik İmha, tüm Kişisel Veriler için 6 aylık zaman aralıklarında gerçekleştirilir. Periyodik İmha sırasında baz alınacak yasal saklama ve İmha süreleri, Veri Envanteri’nde ve işbu Politika’da belirlenmiştir. Şirket, Yönetmelik madde 11(4) kapsamında Kurul’un süreleri kısaltması durumunda, yeni sürelere uyum sağlayacağını taahhüt eder. Silinen, Yok Edilen ve Anonim Hale Getirilen verilere ilişkin işlemlerin diğer hukuki yükümlülüklerden ari en az 3 yıl süre ile saklanır. Şirket’in diğer hukuki yükümlülüklerden kaynaklanan Kişisel Veri saklama hakları saklıdır.

**10.2. Saklama Süreleri**

|  |  |  |
| --- | --- | --- |
| **VERİ SAHİBİ** | **VERİ KATEGORİSİ** | **VERİ SAKLAMA SÜRESİ** |
| Çalışan | İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri | Hizmet akdinin devamında ve hitamından itibaren de 5 yıl müddetle muhafaza edilir. |
| Çalışan | İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri | Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 5 yıl yıl müddetle muhafaza edilir. |
| Çalışan | İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler | Hizmet akdinin devamında ve hitamından itibaren mevzuat gereği 15 (onbeş) yıl müddetle muhafaza edilir. |
| İş Ortağı/Çözüm Ortağı/Danışman | İş Ortağı/Çözüm Ortağı/Danışman ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri | İş Ortağı/Çözüm Ortağı/Danışmanın, Şirket'le olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |
| Ziyaretçi | Şirket'e ait fiziki mekana girişte alınan Ziyaretçi'ye ait ad, soyad, T.C.K.N., araç plakası ile  kamera kayıtları, | 1 yıl süre ile saklanır. |
| İnternet Sitesi Ziyaretçisi | İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri | 1 yıl süre ile saklanır. |
| Çalışan Adayı | Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler | En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır. |
| Stajyer(öğrenci) | Stajyer'e ait staj dosyasında yer alan bilgiler | Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 5 yıl müddetle muhafaza edilir. |
| Müşteri | Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri,  ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri | Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |
| Müşteri | Kamera görüntüleri, araç plaka bilgisi | 1 yıl süre ile saklanır. |
| Potansiyel Müşteri | Potansiyel Müşteri ile Şirket arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, | 1 yıl süre ile saklanır. |
| Şirket’in İşbirliği İçinde Olduğu Kurum/Firmalar  (Tedarikçi, Fason Üretici, Bayi/Franchise) | Şirket’in İşbirliği İçinde Olduğu Kurum/Firmalar ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, Şirket’in İşbirliği İçinde Olduğu Kurum/Firma çalışanı verileri | Şirket’in İşbirliği İçinde Olduğu Kurum/Firmaların, Şirket'le olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır. |

Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

**3.4. PERİYODİK İMHA**

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re’sen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Periyodik imha süreçleri ilk kez 30.06.2018 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

**3.5. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ**

Şirket, gerek talep üzerine gerekse periyodik imha süreçlerinde re’sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

**3.5.1. Teknik Tedbirler**

* Şirket, işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman bulundurur.
* Şirket, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
* Şirket, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
* Şirket, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

**3.5.2. İdari Tedbirler**

* Şirket, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
* Şirket, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
* Şirket, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
* Şirket, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
* Şirket kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.
  1. **Veri Sahiplerinin Talep Etmesi Durumunda Silme ve Yok Etme Süreci**

Veri sahiplerinin Şirket ’e başvurarak kendisine ait Kişisel Verilerin Silinmesini veya Yok Edilmesini talep ettiği durumlarda Şirket, Kişisel Verileri işleme şartlarının mevcut durumunu kontrol eder ve buna bağlı ilgili aksiyonları alır.

Kişisel Verileri İşleme şartlarının tamamı ortadan kalkmışsa talebe konu Kişisel Verileri Siler, Yok Eder veya Anonim Hale Getirir. Şirket, Veri Öznesinin talebini en geç otuz gün içinde sonuçlandırır ve Veri Öznesine bilgi verir.

Kişisel Verileri İşleme şartlarının tamamı ortadan kalkmış ve talebe konu olan Kişisel Veriler üçüncü kişilere aktarılmışsa Veri Sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

Kişisel Verileri İşleme şartlarının tamamı ortadan kalkmamışsa, Şirket ilgili Veri Öznesine gerekçesini açıklayarak talebi reddedebilir ve ret cevabını Veri Öznesine en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirir.

# SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLERİN BİLGİLERİ

Şirket kendi bünyesinde, işbu Politika ve bu Politika ile ilişkili diğer politikaları yönetmek üzere KVK Yetkilisi belirlemiştir. Bu KVK Yetkilisinin görevleri aşağıda belirtilmektedir.

* 1. Kişisel Verilerin korunması ve İşlenmesi ile ilgili temel politikaları hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu’nun onayına sunmak.
  2. Kişisel Verilerin korunması ve İşlenmesine ilişkin politikaların uygulanması ve denetiminin ne şekilde yerine getirileceğine karar vermek ve bu çerçevede şirket içi görevlendirmede bulunmak ve koordinasyonu sağlamak hususlarını Yönetim Kurulu’nun onayına sunmak.
  3. Kanun ve KVK Düzenlemelerine uyumun sağlanması için yapılması gereken hususları tespit etmek ve yapılması gerekenleri Yönetim Kurulu’nun onayına sunmak; uygulanmasını gözetmek ve koordinasyonunu sağlamak.
  4. Kişisel Verilerin korunması ve İşlenmesi konusunda Şirket içerisinde ve Şirket’in iş birliği içerisinde olduğu kurumlar nezdinde farkındalığı arttırmak.
  5. Şirketin Kişisel Veri işleme faaliyetlerinde oluşabilecek riskleri tespit ederek gerekli önlemlerin alınmasını temin etmek; iyileştirme önerilerini Yönetim Kurulu’nun onayını sunmak.
  6. Kişisel Verilerin korunması ve politikaların uygulanması konusunda eğitimler tasarlamak ve icra edilmesini sağlamak.
  7. Kişisel Veri sahiplerinin başvurularını en üst düzeyde karara bağlamak.
  8. Kişisel Veri sahiplerinin; Kişisel Veri işleme faaliyetleri ve kanuni hakları konusunda bilgilenmelerini temin etmek üzere bilgilendirme ve eğitim faaliyetlerinin icrasını koordine etmek.
  9. Kişisel Verilerin korunması ve İşlenmesi ile ilgili temel politikalardaki değişiklikleri hazırlamak ve yürürlüğe koymak üzere Yönetim Kurulu’nun onayına sunmak.
  10. Kişisel Verilerin korunması konusundaki gelişmeleri ve düzenlemeleri takip etmek; bu gelişmelere ve düzenlemelere uygun olarak Şirket içinde yapılması gerekenler konusunda Yönetim Kurulu’na tavsiyelerde bulunmak.
  11. Kurul ve Kurum ile olan ilişkileri koordine etmek.
  12. Yönetim Kurulu’nun Kişisel Verilerin korunması konusunda vereceği diğer görevleri icra etmek.

# POLİTİKA’DA YAPILACAK DEĞİŞİKLİKLER

* 1. İlgili mevzuatta yapılacak her türlü resmi değişikliğin ardından bu değişiklerle uyumlu olacak şekilde Şirket tarafından Yönetim Kurulu onayı ile işbu Politika’da değişiklik yapılabilir. KVK Düzenlemeleri ve işbu Politika arasında bir uyumsuzluk olması halinde KVK Düzenlemeleri esas alınır.
  2. Şirket, Politika üzerinde yapılan değişiklikleri ve incelenebilecek şekilde güncellenen Politika’yı eposta yolu ile çalışanlarıyla paylaşacaktır.

# POLİTİKA’NIN YÜRÜRLÜK TARİHİ

Kişisel Veri Saklama, İmha ve Anonimleştirme Politikası’nın işbu versiyonu 01.11.2019 tarihinde Şirket Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.