

**KVKK-PL-01**

**Kişisel Verileri Saklama ve İmha Politikası**

**DEĞİŞİKLİK KAYITLARI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rev. No** | **Tarih** | **Hazırlayan** | **Değişiklik Nedeni /Sayfa No** | **Onaylayan** | **İmza** |
| 1 |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |
| **4** |  |  |  |  |  |
| **5** |  |  |  |  |  |
| **6** |  |  |  |  |  |
| **7** |  |  |  |  |  |
| **8** |  |  |  |  |  |
| **9** |  |  |  |  |  |

**İçindekiler**

[**DEĞİŞİKLİK KAYITLARI** 2](#_Toc118302613)

[**1.** **TANIMLAR** 5](#_Toc118302614)

[**2.** **POLİTİKA’NIN DAYANAĞI VE AMACI** 6](#_Toc118302615)

[**2.1.** **Dayanak:** 6](#_Toc118302616)

[**2.2.** **Amaç:** 6](#_Toc118302617)

[**3.** **POLİTİKA’NIN KAPSAMI VE DEĞİŞTİRİLMESİ** 6](#_Toc118302618)

[**4.** **KİŞİSEL VERİLERİ İŞLEME FAALİYETLERİNİN ŞARTLARI** 6](#_Toc118302619)

[**5.** **ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ** 7](#_Toc118302620)

[**6.** **KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN GENEL İLKELER** 7](#_Toc118302621)

[**7.** **İŞLENEN KİŞİSEL VERİLER** 8](#_Toc118302622)

[**8.** **KİŞİSEL VERİLERİ TOPLAMA YÖNTEMLERİ** 8](#_Toc118302623)

[**9.** **KİŞİSEL VERİLERİN İŞLENME AMAÇLARI** 8](#_Toc118302624)

[**10.** **KİŞİSEL VERİ VE KAYIT ORTAMI** 9](#_Toc118302625)

[**11.** **KİŞİSEL VERİLERİN AKTARILMASI** 9](#_Toc118302626)

[**11.1.** **Yurtiçi Aktarım:** 9](#_Toc118302627)

[**11.2.** **Yurtdışı Aktarım** 9](#_Toc118302628)

[**11.3.** **Kişisel Verilerin Aktarılabileceği Üçüncü Kişiler:** 9](#_Toc118302629)

[**12.** **KİŞİSEL VERİLERİN GİZLİLİĞİ VE GÜVENLİĞİ** 9](#_Toc118302630)

[**12.1.** **Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Sebepler** 10](#_Toc118302631)

[**12.1.1.** **Kişisel Verilerin Saklanmasını Gerektiren Hukuki, Teknik, İdari ve Diğer Sebepler:** 10](#_Toc118302632)

[**12.1.2.** **Kişisel Verilerin İmhasını Gerektiren Hukuki, Teknik, İdari ve Diğer Sebepler:** 10](#_Toc118302633)

[**12.2.** **Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesinin ve Erişilmesinin Önlenmesi İçin Alınmış Tedbirler** 10](#_Toc118302634)

[**12.2.1.** **Teknik Tedbirler:** 10](#_Toc118302635)

[**12.2.2.** **İdari Tedbirler** 10](#_Toc118302636)

[**12.3.** **Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Tedbirler** 11](#_Toc118302637)

[**12.3.1.** **Teknik Tedbirler:** 11](#_Toc118302638)

[**12.3.2.** **İdari Tedbirler:** 11](#_Toc118302639)

[**12.4.** **Kişisel Verileri Koruma Komitesi** 11](#_Toc118302640)

[**13.** **KİŞİSEL VERİLERİN İMHASI** 11](#_Toc118302641)

[**13.1.** **Kişisel Verilerin Silinmesi:** 12](#_Toc118302642)

[**13.2.** **Kişisel Verilerin Yok Edilmesi:** 13](#_Toc118302643)

[**14.** **KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ** 18](#_Toc118302644)

[**15.** **KİŞİSEL VERİ SAHİBİNİN HAKLARI VE KULLANMA USULLERİ** 18](#_Toc118302645)

[**16.** **Kanun uyarınca Kişisel Verilerin Açık Rıza Olmaksızın İşleyebileceği Haller:** 19](#_Toc118302646)

# TANIMLAR

**Alıcı grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini

**BGA:** BGA Bilgi Güvenliği A.Ş.’yi,

**Doğrudan Tanımlayıcılar:** Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

**Dolaylı Tanımlayıcılar:** Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

**İlgili Kişi:** Kişisel verisi işlenen gerçek kişiyi,

**İlgili Kullanıcı:** Kişisel verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere BGA bünyesinde veya BGA’dan aldığı yetki ve talimatlar doğrultusunda Kişisel Veriler’i işleyen kişileri,

**İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

**Kanun:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu’nu,

**Karartma:** Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri,

**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,

**Kişisel Veri:** BGA’nın faaliyetleri esnasında işletmesel zorunluklar gereği işlediği Veri Envanteri’nde belirtilen kişisel veriler ile özel nitelikli kişisel verileri

**Kişisel Veri İşleme Envanteri:** BGA’nın iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayaran envanteri,

**Kurul:** Kişisel Verileri Koruma Kurulunu,

**Maskeleme:** Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,

**Periyodik İmha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,

**Politika:** İşbu Kişisel Verilerin Saklanması ve İmha Politikası’nı,

**Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

**Kişisel Verileri Anonim Hale Getirme:** Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

**Kişisel Verileri Silme:** Kişisel Veriler’in ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

**Kişisel Verileri Yok Etme:** Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

**Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

**Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan BGA’yı

İfade eder.

# POLİTİKA’NIN DAYANAĞI VE AMACI

* 1. Dayanak: BGA, hukuki ve sosyal sorumluluğunun bir parçası olarak, kişisel ve özel nitelikli kişisel verilerin korunması, işlenmesi ve imha edilmesine ilişkin düzenlemelere uymayı taahhüt etmektedir. İşbu Politika Kanun’un 7. Maddesi ile aynı maddenin 3. Fıkrası atfıyla 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete’de yayınlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca hazırlanmış olan işbu Politika veri koruma, işleme ve imha ile ilgili yasal mevzuatta kabul edilen temel ilkelere dayanmaktadır.
  2. Amaç: İşbu Politika’nın amacı, veri sorumlusu sıfatını haiz BGA tarafından işlenen Kişisel Verilerin ulusal mevzuata, BGA’nın başta Gizlilik ve Bilgi Güvenliği olmak üzere politika, prosedür ve yönetmeliklerine uygun bir biçimde işlenmesi, korunması ve imhasına ilişkin süreçlerin belirlenmesidir.

# POLİTİKA’NIN KAPSAMI VE DEĞİŞTİRİLMESİ

İşbu Politika BGA’ya ait www.bga.com alan adlı web sitesinde yayınlandığı tarihte yürürlüğe girer, mevzuatın öngördüğü değişiklikler, BGA’nın başkaca politika, prosedür, yönetmelikleri yahut Kişisel Veri işleme süreçlerinde meydana gelebilecek değişiklikler ve sair nedenlerle güncellenebilir. Güncellenen Politika web sitesinde yayınlandığı tarihten itibaren geçerli hale gelir.

# KİŞİSEL VERİLERİ İŞLEME FAALİYETLERİNİN ŞARTLARI

Kişisel Verilerin işlenmesi, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder.

Kişisel Veriler, Kanun’un 5. maddesi uyarınca ilgili kişinin açık rızası olmaksızın işlenemez. Ancak yine aynı maddenin düzenlemesi gereği; aşağıdaki şartlardan birinin varlığı hâlinde, İlgili Kişi’nin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

* Kanunlarda açıkça öngörülmesi,
* 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,
* Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
* Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
* İlgili Kişi’nin kendisi tarafından alenileştirilmiş olması,
* Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
* İlgili Kişi’nin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

# ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

Özel nitelikli kişisel veriler Kanun’un 6. Maddesi ile sınırlı sayıda belirlenmiş olup bu kapsamda özel nitelikli kişisel veriler, 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 özel nitelikli kişisel veridir. BGA, Kanun’da açıkça öngörülen haller (sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.) dışında özel nitelikli kişisel verileri İlgili Kişi’nin rıza olmaksızın işlememektedir. İşlenen özel nitelikli kişisel verilere ilişkin güvenliğin sağlanmasına ve imhasına yönelik olarak Kanun ve Yönetmelik maddelerine uyumlu şekilde işbu Politika’nın 12. Maddesinde belirtilen idari ve teknik tedbirleri almıştır.

# KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN GENEL İLKELER

BGA, kişisel veriler ve özel nitelikli kişisel verileri işlerken Kanun’un 4. Maddesi ile öngörülmüş olan aşağıdaki ilke ve esaslara riayet eder.

* Hukuka ve dürüstlük kurallarına uygun olma.
* Doğru ve gerektiğinde güncel olma.
* Belirli, açık ve meşru amaçlar için işlenme.
* İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
* İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

# İŞLENEN KİŞİSEL VERİLER

BGA’nın faaliyetleri esnasında işletmesel zorunluluklar gereği işlemek zorunda olduğu kişisel veriler ve özel nitelikli kişisel veriler Ek – 1’de yer alan Kişisel Veri İşleme Envanteri ile belirtilmiştir.

# KİŞİSEL VERİLERİ TOPLAMA YÖNTEMLERİ

Kişisel Veri/Kişisel Veriler’iniz; II. Bölüm’de belirtilen amaçlarla; BGA bünyesinde yer alan şirkete gelişiniz esnasında ve/veya öncesinde ve/veya sonrasında; sözlü, yazılı, görsel ya da elektronik ortamda, telefon, sms vb. telekomünikasyon iletişim vasıtalarıyla, gönderdiğiniz mailler (e-postalar), internet sitesi, etkinlik kayıtları, sözlü ve benzeri kanallar aracılığıyla toplanmakta ve fiziki ve dijital ortamda saklanmaktadır.

# KİŞİSEL VERİLERİN İŞLENME AMAÇLARI

BGA tarafından Kişisel Veri/Kişisel Veriler’iniz aşağıdaki amaçlar dahilinde işlenebilecektir:

- Türkiye Cumhuriyeti’nde yürürlükte bulunan Mevzuat’ta yer alan hukuki yükümlülüklerimizi yerine getirme;

- Kişisel Veri/Kişisel Verileriniz’in başkaları tarafından ele geçirilmesini engelleyebilmek adına kimlik tespiti ve doğrulama,

- Şirketimizin iç işleyişi ile günlük operasyonların planlanması ve yönetilmesi,

- Risk yönetimi ve kalite geliştirme aktivitelerinin yerine getirilmesi,

- Yasal ve düzenleyici gereksinimlerin yerine getirilmesi,

- Mevzuat uyarınca kamu kurum ve kuruluşları ile edinilen bilgileri paylaşma ve yanıt verme; düzenleyici ve denetleyici kurumlarla, resmi mercilerin talep ve denetimleri doğrultusunda gerekli bilgilerin temini,

- Sunduğumuz hizmetler karşılığında fatura tanzim etme,

- Şirket sistem ve uygulamalarının veri güvenliği kapsamında tüm gerekli teknik ve idari tedbirlerin alınması,

- Size sunduğumuz ürün/hizmetlerinin geliştirilmesi ve iyileştirilmesi amacıyla ürün/hizmetleri kullanımınızı analiz etme ve verilerinizi saklama, hizmetlerimize ilişkin soru veya şikayetlerinize yanıt verme,

- İlgili Mevzuat gereği saklanması gereken verilerinize ilişkin bilgileri muhafaza etme,

- İç politika ve prensiplerine uyum sağlama,

- Sizlere özel tanıtım ve bilgilendirme faaliyetlerinin yürütülmesi ve faydalanmanızın sağlanması, hizmetlerimize ilişkin olarak bilgilendirme amacıyla sizinle iletişime geçilmesi

- ve bunlarla sınırlı olmaksızın, sunmuş olduğumuz ürün/hizmetlerinin yürütülmesi, geliştirilmesi, finansmanının planlanması ve yönetimi, müşteri memnuniyetinin arttırılması, araştırılması ve bağlı nedenler.

İlgili mevzuat uyarınca elde edilen ve işlenen Kişisel Veri/Kişisel Verileriniz, BGA’ya ait fiziki arşivler ve/veya bilişim sistemlerine nakledilerek hem dijital ortamda hem de fiziki ortamda muhafaza altında tutulabilecektir.

# KİŞİSEL VERİ VE KAYIT ORTAMI

BGA, kişisel verileri, verinin niteliği, işlenme amaçları ve kullanım sıklığı gibi esaslara bağlı olarak çeşitli ortamlara kaydetmektedir. Bu kapsamda kişisel verilerin kaydedildiği ortamlar: kağıt, yazılım, bulut, kartlı geçiş ve güvenlik sistemi ve benzeri çevresel ve fiziksel sistemlere kaydedebilmektedir.

# KİŞİSEL VERİLERİN AKTARILMASI

* 1. Yurtiçi Aktarım:BGA, Kanun’un 4. Maddesinde belirtilen haller saklı olmak kaydıyla İlgili Kişi’nin rızası olmaksızın yurtiçinde üçüncü kişiye aktarım yapmamaktadır.
  2. Yurtdışı Aktarım**:** BGA yurtdışına kişisel veri aktarımı gerçekleştirmemektedir.

Kişisel Verilerin Aktarılabileceği Üçüncü Kişiler:BGA, işbu Politika’nın 9. Maddesinde belirtilen amaçlarla, Kanun, Yönetmelik ve ilgili mevzuat uyarınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmasını sağlayarak, kişisel verileri; 4857 sayılı İş Kanunu ve bağlı mevzuat, 6331 sayılı İşçi Sağlığı ve İş Güvenliği Kanunu ve bağlı mevzuat, 5510 sayılı Sosyal Sigortalar Ve Genel Sağlık Sigortası Kanunu ve bağlı mevzuat, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve bağlı mevzuat, 6102 sayılı Türk Ticaret Kanunu ve bağlı mevzuat, 213 sayılı Vergi Usul Kanunu ve bağlı mevzuat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve bağlı mevzuat ve ilgili diğer mevzuat hükümlerinin izin verdiği kişi/kurum ve/veya kuruluşlar; iş ortakları; faaliyetlerimizi yürütmek üzere sözleşmesel olarak hizmet aldığımız ve/veya hizmet verdiğimiz; bankalar, sigorta şirketleri, finans kuruluşları, danışmanlar, denetçiler, işbirliği yaptığımız, yurt içi/yurt dışı kuruluşlar ile diğer gerçek ve/veya tüzel üçüncü kişilere aktarabiliriz.

* 1. KİŞİSEL VERİLERİN GİZLİLİĞİ VE GÜVENLİĞİ

BGA, kişisel verilerini gizliliğini ve güvenliğini önemsemekte, kişisel verilerin güvenliğini sağlayabilmek adına Veri Sorumlusu sıfatıyla alması gereken yeterli idari ve teknik tedbirleri almaktadır. Bu kapsamda;

## **Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Sebepler**

* + 1. **Kişisel Verilerin Saklanmasını Gerektiren Hukuki, Teknik, İdari ve Diğer Sebepler:** Kişisel verilerin toplama amaçlarının veya işletmesel zorunlulukları gereğinde işleme zorunluluğunun ortadan kalkması yahut yasal mevzuatın öngördüğü saklama sürelerini sona ermesi halinde ortaya çıkan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi süreçleri kapsamında imha süreçleri işletilinceye kadar Kişisel Veri İşleme Envanteri’nde öngörülen süreler boyunca saklanmaktadır.
    2. **Kişisel Verilerin İmhasını Gerektiren Hukuki, Teknik, İdari ve Diğer Sebepler:** kişisel verilerin işlenmesini gerektiren amaçların ve saklama sebeplerinin ortadan kalkması, kişisel veri işlemenin açık rıza şartına bağlandığı hallerde İlgili Kişi’nin açık rızasını geri alması, İlgili Kişi’nin Kanun’un 11. Ve Politika’nın 16. Maddeleri kapsamında kişisel verilerinin imhasını talep etmesi ve başvurusunun mevzuat kapsamında kabul edilebilir olması halinde, Kurul kararına dayalı olarak, yasal mevzuatta öngörülen saklama sürelerinin sona ermesi halinde kişisel veriler Politika’nın 13. Maddesinde öngörülen yöntemlerle İmha edilir.

## **Kişisel Verilerin Güvenli Bir Şekilde Saklanması ile Hukuka Aykırı Olarak İşlenmesinin ve Erişilmesinin Önlenmesi İçin Alınmış Tedbirler**

* + 1. **Teknik Tedbirler:** Kanun, Yönetmelik ve Kurul kararları ile belirlenmiş olan yeterli güvenlik tedbirlerinin temini kapsamında kişisel verilere erişim yetkileri sınırlandırılmakta ve erişim kayıtları tutulmaktadır, kişisel verilere BGA içerisinden ve/veya dışarıdan hukuka aykırı bir müdahalenin önlenmesi için veri kayıt ortamları virüs, saldırı, ekran izleme, güvenlik duvarı programları başta olmak üzere çeşitli yazılımlar ve donanımlar ile korunmaktadır, kişisel verilerin hukuka aykırı olarak işlenmesini önleyici düzenli denetimler yaptırılmaktadır, veri kayıt ortamları, düzenli aralıklarla uzman kuruluşlar tarafından güvenlik testlerine tabi tutulmakta; tespit edilen açıklar giderilmektedir.
    2. **İdari Tedbirler:** Kişisel verilerin hukuka uygun olarak işlenmesini temin etmek ve süreçleri takip etmek amacıyla BGA bünyesinde Kişisel Verileri Koruma Komitesi oluşturulmuştur, BGA çalışanları belirli aralıklarla bilgi güvenliği ve Kanun kapsamında eğitimlere tabi tutulmaktadır, işlenen kişisel veriler departman bazında özelleştirilmiş ve ilgili departmanların iş süreçleri kapsamında uyulması gereken özel kurallar belirlenmiştir, şirket içerisinde kişisel verilerin korunmasına ilişkin düzenli denetimler yaptırılmaktadır, çalışanlarla ve 3. Kişilerle imzalanan sözleşmeler kişisel verilerin hukuka uygun işlenmesini ve aykırılık halinde yaptırım uygulanmasını temin etmeye yönelik haldedir.

## **Kişisel Verilerin Hukuka Uygun Olarak İmha Edilmesi İçin Alınmış Tedbirler**

* + 1. **Teknik Tedbirler:** İmha süreçleri, yeterli güvenlik tedbiri alınmış otomatize edilmiş sistemlerle gerçekleştirilmekte ve logları kayıt altında tutulmaktadır. Tüm süreçler alanında bilgi ve tecrübe sahibi uzman teknik personel tarafından gerçekleştirilmektedir.
    2. **İdari Tedbirler:** İmha süreçlerinde kullanılmakta olan otomatize edilmiş sistemlerin güncelliği, çalışır durumda olduğu Kişisel Verileri Koruma Komitesi tarafından takip edilmekte, personele gerekli eğitimler verilmektedir. Şirket içerisinde İmha süreçlerinin hukuka uygun gerçekleştirildiğinin kontrolü için düzenli denetimler yaptırılmaktadır. Tüm sözleşmelerde hukuka uygun hareket edilmesini temin etmeye yönelik maddeler bulunmaktadır.

## **Kişisel Verileri Koruma Komitesi**

BGA, kişisel verilerin hukuka uygun işlenmesi ve İmha süreçlerinin takibini sağlamak amacıyla Kişisel Verileri Koruma Komitesi kurmuştur. Komitenin görevleri:

* Kişisel verilerin işlenmesi süreçlerinde Kanun’un öngördüğü şartların yerine getirilmesini sağlamak, gerekli politika, prosedür ve süreçleri hazırlamak/hazırlatmak
* Kişisel Verilerin hukuka uygun işlenmesi ve imhasını temin etmeye yönelik olarak şirket içi denetimler yapmak ve/veya yaptırmak ve denetimler sonucunda tespit edilen risklerin giderilmesi için gerekli önlemleri sağlamak
* Kişisel verilerin hukuka uygun işlenmesi ve imhası ile hukuka aykırı erişimin önlenmesi amacıyla çalışanların bilgilendirilmesini sağlamak, eğitimler düzenlemek bu eğitimleri belirli aralıklarla tekrar etmek
* İlgili kişilerin başvurularını değerlendirmek, incelemek ve Kanun’da öngörülen süreler içerisinde cevaplanmasını temin etmeye yönelik süreçleri takip etmek, İlgili Kişi’ye cevap vermek
* Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası mevzuatı takip etmek ve/veya ettirmek, yeni düzenlemelerin gerekliliklerini sağlamaya yönelik koordinasyonu sağlamak
* Veri Sorumlusu irtibat Kişisi aracılığıyla Kurul ile iletişim sağlamak, gerekli durumlarda Kurul’a ve bilgi vermek
* Ve bunlarla sınırlı olmaksızın Kişisel verilerin korunmasına ilişkin tüm süreçleri takip etmek.

# KİŞİSEL VERİLERİN İMHASI

Kanun’un 7. Maddesi ile aynı maddenin 3. Fıkrası atfıyla 28 Ekim 2017 tarihli ve 30224 sayılı Resmi Gazete’de yayınlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

BGA, istisnai haller dışında elektronik ortamda tutulan kişisel veriyi (Kanunlarda aksi öngörülmesi, İlgili Kişi’nin başka bir yöntem uygulanmasını seçmesi vb.) işbu seçimlik haklarından Silme yöntemini kullanarak Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebepleri ortadan kalkan kişisel verileri resen veya ilgili kişinin talebi üzerine veri sorumlusu olarak siler.

BGA, istisnai haller dışında kağıt ortamında tutulan kişisel veriyi Yok etme yöntemi kullanarak Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebepleri ortadan kalkan kişisel verileri resen veya ilgili kişinin talebi üzerine veri sorumlusu olarak yok eder.

Silinmiş veya yok edilmiş kişisel verinin bilgisi gerektiğinde yetkili mercilerle paylaşılması amacıyla **ISO-BGYS-PR-10-FR-02 Veri İmha Formu** ile kayıt altına alınır.

* 1. Kişisel Verilerin Silinmesi:BGA, gerekli her türlü teknik ve idari tedbiri alarak kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesini sağlar. Bu işlemi yaparken aşağıdaki süreçleri takip eder:



**Kişisel verilerin silinme yöntemleri:** Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekmektedir. BGA, verinin bulunduğu ortama göre:

* Hizmet Olarak Uygulama Türü Bulut Çözümleri: Bulut sisteminde veriler silme komutu verilerek silinmektedir. Anılan işlem gerçekleştirilirken İlgili Kullanıcı’nın bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmektedir.
* Kağıt Ortamında Bulunan Kişisel Veriler: Kağıt ortamında bulunan kişisel veriler Karartma yöntemi kullanılarak silinmektedir. 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 ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.
* Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması işlemidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilmektedir.
* Taşınabilir Medyada Bulunan Kişisel Veriler: Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmakta ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.
* Veri Tabanları: Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmektedir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmektedir.
  1. Kişisel Verilerin Yok Edilmesi: İstisnai hallerde (Kanunlarda aksi öngörülmesi, İlgili Kişi’nin başka bir yöntem uygulanmasını seçmesi vb.) kişisel verilerin yok edilirken, verilerin bulunduğu tüm kopyaların tespit edilir ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçı kullanılarak tek tek yok edilir:
* Yerel Sistemler: Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir.
  + De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
  + Fiziksel Yok Etme: Optik medya 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. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.
  + Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1’lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.
* Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır:
  + Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Yerel Sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
  + Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da Yerel Sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
  + Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir.
  + Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir.
  + Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Yerel Sitemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
  + Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmektedir.
  + Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre Yerel Sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
  + Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Yerel Sistemler belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
* Kağıt ve Mikrofiş Ortamları: Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortam yok edilmektedir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünür.

Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel veriler ise bulundukları elektronik ortama göre Yerel Sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.

* Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilir.
* Yukarıdaki ortamlara ek olarak; arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:
  + İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin Yerel Sistemler için belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir
  + Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamı sökülerek saklanır, arızalı diğer parçalar üretici, satıcı, servis gibi üçüncü kurumlara gönderilir,
  + Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak BGA dışına çıkartmasının engellenmesi için gerekli önlemlerin alınır.

**13.3.** Kişisel Verilerin Anonim Hale Getirilmesi: BGA İstisnai hallerde (Kanunlarda aksi öngörülmesi, İlgili Kişi’nin başka bir yöntem uygulanmasını seçmesi vb.) kişisel verileri anonim hale getirirken gerekli her türlü teknik ve idari tedbirleri alarak verinin niteliği, büyüklüğü, fiziki ortamlarda bulunma yapısı, çeşitliliği, veriden sağlanmak istenen fayda / işleme amacı, verinin işlenme sıklığı, aktarılacağı tarafın güvenilirliği, anonim hale getirilmesi için harcanacak çabanın anlamlı olması, anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı, dağıtıklık/merkezilik oranı, kullanıcıların ilgili veriye erişim yetki kontrolü, anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali gibi hususları göz önünde bulundurarak aşağıdaki usul, esas ve yöntemlerle gerçekleştirilir.

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

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Anonim Hale Getirme Yöntemleri:

* Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar
  + Değişkenleri Çıkartma: Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.
  + Kayıtları Çıkartma: Bu yöntemde veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.
  + Bölgesel Gizleme: Bölgesel gizleme yönteminde amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer “bilinmiyor” olarak değiştirilir.
  + Genelleştirme: İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkansız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.
  + Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.
  + Global Kodlama: Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.
  + Örnekleme: Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır.
* Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri: Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.
  + Mikro Birleştirme: Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.
  + Veri Değiş Tokuşu Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiflerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.
  + Gürültü Ekleme Bu yöntem ile, seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkartmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.
* Anonim Hale Getirmeyi Kuvvetlendirici İstatistiksel Yöntemler: Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.
  + K-Anonimlik: Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. 28 K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilmesiyle oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.
  + L-Çeşitlilik: K-Anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır. Her bir grubun içinde belli bir çeşitlilik yaratılmasına dikkat edilerek maskeleme yöntemi kullanılmaktadır.
  + T-Yakınlık: L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denilmektedir.



# KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

BGA’nın işletmesel faaliyetleri kapsamında işlemek zorunda olduğu kişisel verileri saklama ve imha süreleri KVKK-DOK-07 Kişisel Veri Envanteri’nde belirtilmektedir. İmha süresi dolmuş kişisel verilerin tespiti için Periyodik İmha Süresi Kurul tarafından telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması nedenleriyle kısaltılmadığı takdirde 6 (altı) aydır.

# KİŞİSEL VERİ SAHİBİNİN HAKLARI VE KULLANMA USULLERİ

Kişisel Veri/Kişisel Veriler’inizin BGA tarafından Veri Sorumlusu sıfatı ile işlendiği ölçüde KVKK'nın 11. maddesi gereği, aşağıda yer alan “**KVKK-DOK-02-FR-01 Kişisel Veri Bilgi Talep Formu**"nu doldurup şirket merkez adresine **(İçerenköy Mah. Umut Sk. Quick Tower No:10-12 Kat:12 İç Kapı No:55 Ataşehir – İstanbul**) elden teslim ederek, noter kanalıyla göndererek, şahsınıza ait güvenli elektronik imza ile imzalanmış bir e-posta ile mail atarak yahut yine güvenli elektronik imza ile imzalanmış bir “Word veya PDF” uzantılı dosyayı **kvkk@bga.com** adresine e-posta ile göndererek;

Herhangi bir Kişisel Veri/Kişisel Veriler’inizin işlenip işlenmediğini öğrenme,

Kişisel Veri/Kişisel Veriler’inizin işlenme faaliyetlerine ilişkin olarak bilgi talep etme,

Kişisel Veri/Kişisel Veriler’inizin işlenme amaçlarını öğrenme,

Kişisel Veri/Kişisel Veriler’inizin yurt içinde veya yurt dışında üçüncü kişi/kurum ve/veya kuruluşa aktarılmış olması durumunda bu kişileri/kurum ve/veya kuruluşları öğrenme,

Kişisel Veri/Kişisel Veriler’inizin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini/güncellenmesini isteme,

Kişisel Veri/Kişisel Veriler’inizin işlenmesini gerektiren sebeplerin ortadan kalkması veya BGA’nın söz konusu verileri işleyebilmek için hukuki dayanağı veya meşru menfaatinin bulunmaması halinde Kişisel Veri/Kişisel Veriler’inizin silinmesini veya yok edilmesini isteme,

Kişisel Veri/Kişisel Veriler’inizin otomatik sistemler vasıtasıyla işlenmesi sonucu ortaya çıkabilecek aleyhte sonuçlara itiraz etme ve,

Kişisel Veri/Kişisel Veriler’inizin kanuna aykırı bir şekilde işlenmesi sebebiyle zarara uğramanız halinde bu zararın tazmin edilmesini isteme hakkına sahipsiniz.

BGA, talebin niteliğine göre talebi en kısa sürede ve en geç otuz gün içinde ücretsiz olarak yahut Kişisel Verileri Koruma Kurulu tarafından belirlenen tarifedeki ücret mukabilinde sonuçlandıracaktır. Bu halde başvurunun BGA’nın hatasından kaynaklanması hâlinde alınan ücret iade edilir.

# Kanun uyarınca Kişisel Verilerin Açık Rıza Olmaksızın İşleyebileceği Haller:

Kanun’un 5. maddesi uyarınca, aşağıdaki hallerde açık rızanız aranmaksızın kişisel veriler işlenebilmektedir.

* Kanunlarda açıkça öngörülen hallerde,
* Fiili imkânsızlık nedeniyle veri sahibi olarak rızanızı açıklayamayacak durumda olmanız veya rızanıza hukuki geçerlilik tanınmayan hallerde kendinizin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verinizin işlenmesinin zorunlu olması,
* Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait Kişisel Veri/Kişisel Veriler’inizin işlenmesinin gerekli olması,
* Bir hukuki yükümlülüğün yerine getirilebilmesi için zorunlu olması,
* Kişisel Veri/Kişisel Veriler’inizin tarafınızca alenileştirilmiş olması,
* Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
* Sahip olduğunuz temel hak ve özgürlüklerinize zarar vermemek kaydıyla, BGA’nın meşru menfaatleri için veri işlenmesinin zorunlu olması.

**Ek – 1: KVKK-DOK-07 Kişisel Veri Envanteri**

**Ek – 2: KVKK-DOK-02-FR-01 Kişisel Veri Bilgi Talep Formu**