KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

VERİ SORUMLUSU KİMLİĞİ

UNVAN: BİES GLOBAL DENETİM DANIŞMANLIK YAZILIM VE EĞİTİM HİZMETLERİ LİMİTED ŞİRKETİ

VERGİ NO: 1700499024

TELEFON: 5322048486

KEP:

E-POSTA: info@biesglobal.com.tr

SUBDOMAIN: biesglobal.kvksis.com

ADRES: ERCIYES TEKNOPARK TGB YILDIRIM BEYAZIT MAH. NO. 5-55[county][city]

MADDE 1: AMAÇ
Kişisel verileri saklama ve imha politikası yukarıdaki tabloda bilgileri yer alan Veri Sorumlusu tarafından işlenen kişisel verilerin saklanması ve imhasına yönelik iş ve işlemler konusundaki usulleri ve esasları belirlemek amacıyla hazırlanmıştır.
MADDE 2: KAPSAM
Şirket çalışanlarına, çalışan adaylarına, ürün ve hizmet alıcısı kişilere, potansiyel ürün ve hizmet alıcılarına, ziyaretçilere, tedarikçilere ve ait kişisel veriler bu politika kapsamındadır.
Şirketin sahip olduğu ya da şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu politika uygulanır.
MADDE 3: TANIMLAR
Alıcı grubu : Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
Açık rıza : Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme : Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
Çalışan : Şirket personeli
Elektronik ortam : Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlar
Elektronik olmayan ortam : Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar
Hizmet sağlayıcı : Şirket ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
İlgili kişi : Kişisel verisi işlenen gerçek kişi
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 kişiler
İmha : Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
Kanun : 6698 Sayılı Kişisel Verilerin Korunması Kanunu
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 ortam
Kişisel veri : Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel veri işleme envanteri : Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kurul : Kişisel Verileri Koruma Kurulu
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
Periyodik imha : 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 işlemi
Politika : Kişisel Verileri Saklama ve İmha Politikası
Şirket : BİES GLOBAL DENETİM DANIŞMANLIK YAZILIM VE EĞİTİM HİZMETLERİ LİMİTED ŞİRKETİ
Ürün ve hizmet alıcısı : Müşteri
Veri işleyen : Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri kayıt sistemi : Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri sorumlusu : Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi
Veri sorumluları sicil bilgi sistemi : Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi
VERBİS : Veri Sorumluları Sicil Bilgi Sistemi
Yönetmelik : 28 Ekim 2017 tarihli Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

MADDE 4: SORUMLULUK VE GÖREVLER

Şirketin tüm çalışanları ve birimleri; kişisel verilerin hukuka uygun olarak elde edilmesi, işlenmesi ve saklanması konusunda sorumlu birimlere tam ve aktif destek verir. Politika kapsamında alınan idari ve teknik tedbirlerin uygulanmasında, birim

çalışanlarının eğitilmesinde, çalışanların farkındalığının sağlanmasında, artırılmasında ve izlenmesinde, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesinde ve kişisel verilerin hukuka uygun olarak muhafazasında tüm çalışanlar ve birimler, sorumlu birimlere destek olur.

MADDE 5: KAYIT ORTAMLARI

Kişisel veriler, şirket tarafından EK TABLO: 1'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde muhafaza edilir.

MADDE 6: SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Şirkette, faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar ve kanun ile ilgili mevzuat kapsamında muhafaza edilir. Bu kapsamda saklamayı gerektiren sebepler şunlardır:

- Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması nedeniyle saklanması,
- Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması
- Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla şirketin meşru menfaatleri için saklanmasının zorunlu olması
- Kişisel verilerin şirketin herhangi bir hukuki yükümlülüğünü yerine getirmesi amacıyla saklanması
- Mevzuatta kişisel verilerin saklanmasının açıkça öngörülmesi
- Veri sahiplerinin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından veri sahiplerinin açık rızasının bulunması

MADDE 7: SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Şirket aşağıdakiler dahil olmak ancak bununla sınırlı olmamak üzere, ilgili kişinin veya ilgili kişi tarafından belirtilen üçüncü tarafların kişisel verilerini çeşitli amaçlarla işleyebilir:

- Çalışanlar için iş akdi ve mevzuattan kaynaklı yükümlülüklerin yerine getirilmesi
- Mal hizmet satın alım süreçlerinin yönetilmesi
- Hukuk işlerinin takibi ve yürütülmesi
- Faaliyetlerin mevzuata uygun yürütülmesi
- Ürün hizmetlerin pazarlama süreçlerinin yürütülmesi
- Mal ve hizmet satış sonrası destek hizmetlerinin yürütülmesi
- İletişim faaliyetlerinin yürütülmesi
- Çalışanlar için yan haklar ve menfaatleri süreçlerinin yürütülmesi
- Mal hizmet satın alım süreçlerinin yönetilmesi
- Ziyaretçi kayıtlarının oluşturulması ve takibi
- İş sağlığı güvenliği faaliyetlerinin yürütülmesi
- Yetkili kişi kurum ve kuruluşlara bilgi verilmesi
- Hizmetin ifası
- Fiziksel mekân güvenliğinin sağlanması

MADDE 8: İMHAYI GEREKTİREN HUKUKİ SEBEPLER

Kişisel veriler, aşağıdaki durumların varlığı halinde ilgili kişinin talebi üzerine veya re'sen şirket tarafından silinir ya da yok edilir:

- Kişisel verinin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya kaldırılması
- Kişisel verinin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması
- Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması

MADDE 9: TEKNİK TEDBİRLER

Veri Sorumlusu tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıdadır:

- Güncel anti-virüs sistemleri kullanılır
- Şifreleme yapılır
- Taşınabilir bellek, CD, DVD ortamında aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılır
- Kişisel verilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanır
- Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli yöntemler ile korunur

MADDE 10: İDARİ TEDBİRLER

Veri Sorumlusu tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıdadır:

- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik tedbirlerinin alınır
- Kişisel veri içeren fiziksel ortamların dış risklere karşı güvenliğinin sağlanır
- Kişisel veri içeren ortamların güvenliğinin sağlanır
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri bulunur
- Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır
- Gizlilik taahhütnameleri yapılmıştır
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin iptali yapılır
- İmzalanan sözleşmeler veri güvenliği hükümleri içerir
- Kişisel veri güvenliğinin takibi yapılır
- İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.

MADDE 11- KİŞİSEL VERİLERİN SİLİNMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 2'te belirtilen yöntemlerle silinir.

MADDE 12- KİŞİSEL VERİLERİN YOK EDİLMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 3'te belirtilen yöntemlerle yok edilir.

MADDE 13: KİŞİSEL VERİLERİN ANONİMLEŞTİRİLMESİ YÖNTEMLERİ

Kişisel veriler EK TABLO: 4'te belirtilen yöntemlerle anonimleştirilir.

MADDE 14: SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından kişisel verilerin saklama süresi belirlenirken; öncelikle yasal mevzuatta söz konusu kişisel verinin saklanmasına ilişkin olarak bir süre öngörülmüş

ise bu süreye riayet edilir. Bunun haricinde; EK TABLO: 5'te yer alan saklama ve imha süresi tablosu esas alınır.

MADDE 15: PERİYODİK İMHA SÜRESİ

Her yıl ..... ve ..... Aylarında periyodik imha işlemi gerçekleştirilir.

MADDE 16: POLİTİKANIN YAYIMLANMASI, SAKLANMASI VE GÜNCELLENMESİ

Politika, ıslak imzalı (basılı kâğıt) olarak yayımlanır ve basılı kâğıt nüshası şirket bünyesinde saklanır. Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli bölümler güncellenir.

MADDE 17: YÜRÜRLÜK

Politika, şirketin yetkilisince imza edilmesinin ardından yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, politikanın ıslak imzalı eski nüshaları iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile şirket tarafından saklanır.

EK TABLO: 1 Kişisel Veri Saklama Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Kişisel bilgisayarlar, mobil cihazlar, yazıcılar, tarayıcılar, fotokopi makineleri, çıkarılabilir ve taşınabilir bellekler, bulut veri depolama alanları	Kağıtlar, yazılı ve basılı ortamlar, görsel kayıtlar, manuel veri kayıt sistemleri, klasörler/arşiv

EK TABLO: 2 Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Silinme Yöntemi
Elektronik ortam	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.
Fiziksel ortam	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu kişi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir medya	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, şirket sahibi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

EK TABLO: 3 Kişisel Verilerin Yok Edilmesi Yöntemleri

Veri Kayıt Ortamı	Yok Edilme Yöntemi
Fiziksel Ortam	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, evrak imha makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik ya da manyetik medya	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

EK TABLO: 4 Anonimleştirme

Değişkenleri çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının 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 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. 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.

EK TABLO: 5 Saklama ve İmha Süresi Tablosu

Sıra No:	Veri kategorisi	Veriyi içeren belge	Saklama Süresi	İmha Süresi
1	Ceza mahkûmiyeti ve güvenlik tedbirleri	Adli sicil kaydı	İş ilişkisinin bitimini takiben 1 yıl	Saklama süresinin bitimini takiben 180 gün
2	Felsefi inanç, din, mezhep ve diğer inançlar	Nüfus cüzdanı örneği	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
3	İletişim	Formlar, İş sözleşmeleri	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
4	Kimlik	Nüfus cüzdanı örneği, Aile durum bildirimi, Vesikalık fotoğraf, Gizlilik taahhütnameleri, İş sözleşmeleri	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
5	Mesleki deneyim	Aile durum bildirimi, Diploma ve sertifikalar	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
6	Finans	Aile durum bildirimi, ücret bordroları, İş sözleşmeleri	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün

7	Sağlık bilgileri	Sağlık raporu	İş ilişkisinin bitimini takiben 10 yıl / İş sağlığı ve güvenliği nedeniyle alınan raporlarda iş ilişkisinin bitimini takiben 15 yıl / Hasta, Veli, Vasi, Temsilci 'den elde edilmesini takiben 20 yıl	Saklama süresinin bitimini takiben 180 gün
8	Özlük	Nüfus cüzdanı örneği, Askerlik durum belgesi	İş ilişkisinin bitimini takiben 10 yıl	Saklama süresinin bitimini takiben 180 gün
9	Özgeçmiş	Özgeçmiş	İş ilişkisinin bitimini takiben 1 yıl	Saklama süresinin bitimini takiben 180 gün
10	Fiziksel mekân güvenliği	Kamera kayıtları	Elde edilmesini takiben 2 ay / CCTV Kayıtları 90 Gün	Saklama süresinin bitimini takiben 7 gün