BURSA TEKNOLOJİ ORGANİZE SANAYİ BÖLGESİ
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

İÇİNDEKİLER

BURSA TEKNOLOJİ ORGANİZE SANAYİ BÖLGESİ
KİŞİSEL VERİ SAKLAMA ve İMHA POLİTİKASI

1. BÖLÜM

GİRİŞ, POLİTİKA'NIN AMACI, KAPSAMI VE TANIMLAR

1.1 GİRİŞ, POLİTİKA'NIN AMACI

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), Bursa Teknoloji Organize Sanayi Bölgesince ("Bölge") gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

Bölge; Kişisel Verilerin İşlenmesi ve Korunması Politikasında belirlenen misyon, vizyon ve temel ilkeler doğrultusunda; Bölge çalışanları, çalışan adayları, hizmet sağlayıcıları, hizmet alanlar, hissedarlar, tedarikçiler, yüklenici ve altyükleniciler, katılımcılar, kiracılar, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin T.C. Anayasası, uluslararası sözleşmeler, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") ve diğer ilgili mevzuata uygun olarak işlenmesini ve ilgili kişilerin haklarını etkin bir şekilde kullanmasının sağlanmasını öncelik olarak belirlemiştir.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Bölge tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 POLİTİKA'NIN KAPSAMI

Bölge çalışanları, çalışan adayları, hizmet sağlayıcıları, hizmet alanlar, katılımcılar, hissedarlar, tedarikçiler, yüklenici ve altyükleniciler, kiracılar, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Bölgenin sahip olduğu ya da Bölgece yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3 TANIMLAR

Bu politikada geçen;

Hizmet Sağlayıcı: Bursa Teknoloji Organize Sanayi Bölgesi ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişiyi,

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,

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

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 İşleme Envanteri : Veri sorumlularının 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 envanteri,

Katılımcılar / Kiracılar: Bölge ile sözleşmesel ilişki kapsamında arsa tahsis edilen katılımcılar ve katılımcıların kiracıları,

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

Veri Sorumluları Sicil Bilgi Sistemi : Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili Bilgi Sistemi diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini,

VERBİS : Veri Sorumluları Sicil Bilgi Sistemini,

İfade eder.

Bu politikada yer almayanlar tanımlar için, Kanundaki tanımlar geçerli olacaktır.

2.BÖLÜM

SORUMLULUK VE GÖREV DAĞILIMLARI

Bölge'nin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir. İlgili disiplin sürecine ilişkin usul ve esaslar Disiplin Prosedürü'nde yer almaktadır.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Saklama ve imha süreçleri görev dağılımı

UNVAN	BİRİM	GÖREV
Bilgi İşlem Müdürü	Bilgi İşlem Müdürlüğü	Politika'nın uygulanmasında ihtiyaç duyulan teknikçözümlerin sunulmasından sorumludur.
Hukuk Müşavirliği, İnsan Kaynakları Müdürlüğü, Satın Alma Müdürlüğü, Bilgi İşlem Müdürlüğü	Uyum Ekibi	Görevlerine uygun olarak Politikanın yürütülmesinden sorumludur.

3.BÖLÜM

KAYIT ORTAMLARI

Kişisel veriler, Kurum tarafından Tablo 2'de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

Tablo 2: Kişisel veri saklama ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) Yazılımlar (ofis yazılımları, portal,EBYS, VERBİS.) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) Kişisel bilgisayarlar (Masaüstü, dizüstü) Optik diskler (CD, DVD vb.)	Kağıt Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) Yazılı, basılı, görsel ortamlar

4.BÖLÜM
SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Bölge tarafından; çalışanlar, çalışan adayları, hizmet alanlar, katılımcılar, kiracılar, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ve hissedarlara, tedarikçilere, yüklenici ve altyüklenicilere ait kişisel veriler Kanuna uygun olarak saklanır ve imha edilir.

Bu kapsamda saklama ve imhaya ilişkin detaylı açıklamalara aşağıda sırasıyla yer verilmiştir.

4.1 SAKLAMAYA İLİŞKİN AÇIKLAMALAR

Bölge ve Bölge'nin şube ve temsilciliklerinde kayıt gören, düzenlenen ve dosyalanan her türlü evrak, belge ve defterler ile herhangi bir delil olmaya veya milli veya milletlerarası hukuk, muamele ve münasebetler bakımından herhangi bir hususu aydınlatmaya veya düzenlemeye yarayan her türlü yazılı evrak, defter, resim, plan, program, harita, proje, maket, model, numune, fotoğraf, film, cd, ses ve görüntü bandı, baskı ve benzeri belgeler arşiv malzemesini oluşturur ve bunlar öngörülen süreler içinde muhafaza edilir.

Kanunun 3'üncü maddesinde *kişisel verilerin işlenmesi* kavramı tanımlanmış, 4'üncü maddesinde işlenen kişisel verinin *işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi* gerektiği belirtilmiş, 5 ve 6'ncı maddelerde ise *kişisel verilerin işleme şartları* sayılmıştır. Buna göre, Bölgemiz faaliyetleri çerçevesinde kişisel veriler, *ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.*

Bölge güvenliğin sağlanması ve bu Politika'da belirtilen amaçlarla; Bölge tarafından bina ve tesislerimiz içerisinde kaldığınız süre boyunca talep eden ziyaretçilerimize internet erişimi sağlanabilmektedir. Bu durumda internet erişimlerinize ilişkin log kayıtları 5651 Sayılı Kanun ve bu Kanuna göre düzenlenmiş olan mevzuatın amir hükümlerine göre Bölge güvenliğinin sağlanması ve Politika'da belirtilen amaçlarla; kayıt altına alınmaktadır. Söz konusu bu kayıtlar ancak yetkili kamu kurum ve kuruluşları tarafından talep edilmesi Bursa Teknoloji Organize Sanayi Bölgesi içinde gerçekleştirilecek denetim süreçlerinde ilgili hukuki yükümlülüğümüzü yerine getirmek amacıyla saklanmaktadır.

Bu çerçevede elde edilen log kayıtlarına yalnızca sınırlı sayıda Bölge çalışanının erişimi bulunmaktadır. Bahsi geçen kayıtlara erişimi olan Bölge çalışanları bu kayıtları yalnızca yetkili kamu kurum ve kuruluşundan gelen talep veya denetim süreçlerinde kullanmak üzere erişmekte ve hukuken yetkili olan kişilerle paylaşmaktadır. Kayıtlara erişimi olan sınırlı sayıda kişi gizlilik taahhütnamesi ile eriştiği verilerin gizliliğini koruyacağını beyan etmektedir.

4.1.1 SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

Kurumda, faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 4562 sayılı Organize Sanayi Bölgeleri Kanunu ve ilgili Yönetmelikler
  6098 sayılı Türk Borçlar Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 4734 sayılı Kamu İhale Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar
- Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 sayılı Kamu Mali Yönetimi Kanunu,
  6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4857 sayılı İş Kanunu,
- 2547 sayılı Yükseköğretim Kanunu,
- 2828 sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin
- Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik ve ilgili diğer

kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2 SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

Bölge, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İnsan kaynakları süreçlerini yürütmek.
- Bölgenin kurumsal iletişimini sağlamak.
- Bölge güvenliğini sağlamak,
- İstatistiksel çalışmalar yapabilmek.
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.

- Bölge ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- Yasal raporlamalar yapmak.
- Çağrı merkezi süreçlerini yönetmek.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.2 İMHAYI GEREKTİREN SEBEPLER

Kişisel veriler;

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- İşlenmesini 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 Kurum tarafından kabul edilmesi,
- Bölgenin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

durumlarında, Bölge tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir,yok edilir veya anonim hale getirilir.

5.BÖLÜM

TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanun'un 12'nci maddesiyle Kanun'un 6'ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Bölge tarafından teknik ve idari tedbirler alınır.

5.1 TEKNİK TEDBİRLER

Bölge tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

- Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.

Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Bölge içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.
- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.
- Bölge, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurul'a bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.
- Bölge internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.

5.2 İDARİ TEDBİRLER

Bölge tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmenin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara kişisel verilerin korunmasına ilişkin taahhütname ve gizlilik sözleşmesi imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.

- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6.BÖLÜM

KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, Bölge tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1 KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel veriler Tablo-3'te verilen yöntemlerle silinir.

Tablo 3: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	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 Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler,sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2 KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel veriler, Kurum tarafından Tablo-4'te verilen yöntemlerle yok edilir.

Tablo 4: Kişisel Verilerin Yok Edilmesi

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	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.

6.3 KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

Bölge, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

Kanun'un 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler Kanun kapsamı dışında olup, kişisel veri sahibinin açık rızası aranmayacaktır. Anonim hale getirilerek işlenen kişisel veriler Kanun kapsamı dışında olacağından düzenlenen haklar bu veriler için geçerli olmayacaktır. Bölge tarafından en çok kullanılan anonimleştirme teknikleri aşağıda sıralanmaktadır.

(i) Maskeleme (Masking)

Veri maskeleme ile kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir.

Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, TC Kimlik No vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkânsız hale geldiği bir veri setine dönüştürülmesi.

Kişisel verilerin belli alanlarının silinerek veya yıldızlanarak kişinin belirlenemez hale getirilmesidir.

*Örneğin, kişinin kredi kartı numarasının bir kısmının yıldızlanması durumunda maskeleme söz konusudur. (6698 **** **** 0006)*

(ii) Toplulaştırma (Aggregation)

Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir.

Örnek: Çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

Verilerin kümülatif hale getirilerek toplam değerlerinin yansıtılmasını ifade eder.
Örneğin, şirkette kadın çalışan sayısının Z adet olması ve sayının %40'ının üniversite mezunu, %60'ının yüksek lisans mezunu olmasına ilişkin veriler anonim hâle getirilmiştir.

(iii) Veri Türetme (Data Derivation)

Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır.

Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

Mevcuttaki detay verilerin daha genel karşılıklarıyla değiştirilmesidir.

Örneğin, doğum tarihi bilgisinin Gün/Ay/Yıl detaylarının yerine kişinin direkt yaşının yazılması durumunda veri türetmek suretiyle anonimleştirme yapılmıştır.

(iv) Veri Karma (Data Shuffling, Permutation)

Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır.

Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek hale getirilmesi.

Veri kümesi içinde değerlerin karıştırılarak toplam faydaya zarar vermeden kişilerin tespit edilebilirlik özelliğinin yok edilmesini ifade eder. Yaş ortalaması alınmak istenen bir sınıfta kişilerin yaşlarını gösteren değerlerin birbirleriyle değiştirilmesi durumunda veri karması yapılmıştır.

7. BÖLÜM

SAKLAMA VE İMHA SÜRELERİ

Bölge tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde Bilgi İşlem ve Teknolojileri Müdürlüğünce güncellemeler yapılır.

Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi Bilgi İşlem ve Teknolojileri Müdürlüğü tarafından yerine getirilir.

Tablo 5: Süreç bazında saklama ve imha süreleri tablosu

SÜREÇ/ İŞLEM	SAKLAMA SÜRESİ	İMHA SÜRESİ
Yevmiye defteri hariç muhasebeyleilgili defterler, finansla ilgili evraklar	Hukuki İlişki veya İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Muhasebeyle ilgili fiş, makbuz ve diğer belgeler;	Hukuki İlişki veya İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Gelen ve giden evrak defterleri;	Evrak Kayıt Tarihini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Fiziksel Mekan Güvenliği	Kamera Kaydı Kayıt Tarihi +1Ay/Diğer Kayıtlarda Kayıt Tarihini Takip Eden Yılbaşından İtibaren 2Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Özlük	İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Kimlik, İletişim	İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
İşlem Güvenliği	Kaydın Alındığı Tarihi Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde

Bölge İşlemleri	İlişkinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takipeden ilk periyodik imha süresinde
Görsel ve İşitselKayıtlar	İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15Yıl/Diğerleri İçin Kayıt Tarihi+1Ay	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Bölge İletişim Faaliyetlerinin İcrası	Faaliyetin sona ermesini takiben 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş Sözleşmesinin Sona Ermesini Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Log Kayıt Takip	Kaydın Tutulmasını Takip Eden Yılbaşından İtibaren 15 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. BÖLÜM

PERİYODİK İMHA SÜRESİ

Bölge, periyodik imha süresini 6 ay olarak belirlemiştir.

02.02.2019 tarihli ve 30674 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Organize Sanayi Bölgeleri Uygulama Yönetmeliği gereğince periyodik imha işlemleri gerçekleştirilmektedir.

Muhafaza süresi dolan arşiv malzemesinin tespiti ve imhası işlemlerini yapmak üzere yönetim kurulu kararıyla personelden müteşekkil üç kişilik bir komisyon oluşturulur. Komisyon muhafaza süresi dolan arşiv malzemesini yönetim kurulunca/şube yönetim kurulunca kararlaştırılan süre içerisinde bir liste halinde tespit eder. İki nüsha olarak tanzim edilecek bu listede, arşiv malzemesinin mahiyeti, aidiyeti ve tarihi belirtilir.

Komisyonca tanzim edilen listeler yönetim kurulunun onayına sunulur. Yönetim kurulunca onaylanan listelerde yer alan arşiv malzemesi, komisyonun huzurunda önceden tespit edilecek bir yerde yakılmak veya kağıt sanayi müesseselerine verilmek suretiyle imha edilir.

Yönetim kurulunca imha edilmek üzere onaylanan arşiv malzemesi listesinin bir nüshası kararın içerisine dercedilir veya yönetim kurulu/şube yönetim kurulu karar defterinin kararı takip eden sayfalarına kenarları mühürlenerek yapıştırılır, diğer nüshası da Bölge'de muhafaza edilmek üzere dosyasına konulur.

9. BÖLÜM

VERİ SORUMLUSUNA BAŞVURU VE BÖLGENİN BAŞVURUYA CEVAP VERME USÛLÜ

Bölge'ye kişisel veri işlenmesi faaliyetine ilişkin yapılan başvurularda değerlendirme ve cevaplama usulü "Başvuru ve Cevap Prosedürü"nde düzenlenmiştir. Kişisel veri işlenmesi faaliyetinin usûl ve esaslarına ilişkin ayrıntılı bilgiye Bursa Teknoloji Organize Sanayi Bölgesi Kişisel Verilerin İşlenmesi ve Korunması Politikası'nın 2.4.1 "Veri Sorumlusuna Başvuru Ve Bölgenin Başvuruya Cevap Verme Usûlü" bölümünden ulaşılabilinmektedir.

10. BÖLÜM

POLİTİKANIN GÜNCELLENMESİ, YÜRÜRLÜĞÜ VE DİĞER POLİTİKALAR

İşbu Politika, Kişisel verilerin işlemesi ve korunması politikası ile birlikte yürürlüğe konulmuştur.

Politika, Bölge'nin https://www.teknosab.org.tr internet sitesinde yayımlanır.

İşbu Politika, Bölge'nin bütün birimlerine sistem üzerinden bildirilecek; üyelere, ziyaretçilere ve ilgili diğer kişilere web sitesi veya diğer uygun vasıtalarla duyurulacaktır.

Kişisel verileri işleme faaliyetlerine ilişkin hazırlanan işbu Politika, Bursa Teknoloji Organize Sanayi Bölgesi Kişisel Verilerin İşlenmesi ve Korunması Politikasına ek olup, ayrılmaz parçaları niteliğinde olup, bu politika hükümleri Yönetim Kurulu tarafından yürütülür.