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

1. **AMAÇ**

Bu Kişisel Veri Saklama, İşleme ve İmha Politikası (**“Politika”**), Boston Scientific Tıp Gereçleri Ltd. Şti. (“BSCI”) tarafından gerçekleştirilmekte olan kişisel veri işleme, saklama ve imha faaliyetlerine ilişkin iş ve işlemler ile çalışanlarımızın görevlerini ifa ederken ellerine geçen ya da bilgileri dahiline giren tüm Kişisel Verileri (aşağıdaki tanımlara bakınız) gizli tutmalarını ve Türkiye’de yürürlükte bulunan 6698 sayılı Kişisel Verilerin Korunması Kanunu (Bundan böyle **“KVKK”** olarak anılacaktır.) ve hukuki dayanağını ondan alan ikincil mevzuat ile Kişisel Verileri Koruma Kurulu’nun almış olduğu kararlara (Hepsi birlikte bu doküman içerisinde **“Veri Koruma Mevzuatı”** olarak anılacaktır.) uymalarını sağlamak amacıyla tasarlanmış ve çıkartılmış bulunmaktadır.

1. **KAPSAM**

Bu Politika, görevleri kapsamında Kişisel Verileri tamamen veya kısmen otomatik yol ve araçlarla işleyen ya da bir kayıt sisteminin bir parçasını oluşturan ya da bir kayıt sisteminin bir parçasını oluşturması amaçlanan Kişisel Verileri (otomatik yol ve araçlar dışında) başka yol ve araçlarla işleyen tüm çalışanlarımıza; BSCI çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel verilerin işlenmesi faaliyetlerine ilişkin olarak uygulanır.

1. **TANIMLAR**

**Veri Süjesi ya da İlgili Kişi:** Verinin ait olduğu, kimliği belirlenmiş veya belirlenebilir bir gerçek kişi anlamına gelir.

**Kişisel Veriler:** İsim, adres, telefon numarası, e-posta adresi veya benzeri kimlik bilgileri gibi Veri Süjesiyle ilgili her türlü bilgi anlamına gelir.

**Özel Nitelikli Kişisel Veriler:** Bir kişinin 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 Veri anlamına gelir.

**Kişisel Verilerin İşlenmesi:** 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 işlemdir.

1. **SORUMLULUKLAR**
   1. Veri Koruma Komitesi, Müşteri Hizmetleri, Operasyon, Kalite, Regülasyon, İhale, İnsan Kaynakları ve Eğitim Merkezi departmanlarının her birinden birer üyenin katılımıyla oluşan komitedir. Bu Politikayı ve bu Politikada yapılan tüm revizyon ve değişiklikleri incelemek ve onaylamak Veri Koruma Komitesinin sorumluluğundadır. Veri Koruma Komitesi aynı zamanda Politikayı geliştirmek ve gerekli eğitimleri vermek ile Politikanın yorumlanması konusunda çalışanlara kılavuzluk etmekle görevlidir. Komite ayrıca bu Politikaya uyulup uyulmadığını denetler ve uyulması için gerekli desteği verir.
   2. Veri Koruma Komitesi işbu Politika’nın 12. maddesinde yer alan periyodik imha süreçlerinin kontrolünden, belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, bu sürelerin takibinden ve muhafaza süresi dolan verilerin imha edilmesinden sorumludur. Veri Koruma Komitesi’nin takibinden sorumlu olduğu BSCI periyodik imha süreci 2 yıl olarak belirlenmiştir.
   3. Genel Müdür ve Veri Koruma Komitesinin birlikte yürütmesi gereken görevi, Politikadan sapma ve istisna taleplerini incelemek ve onaylamaktır.
2. **BSCI KİŞİSEL VERİ SAKLAMA VE İŞLEME FAALİYETLERİ**

Aşağıda sayılan iş faaliyetleri sırasında, çalışanlarımız, Kişisel Verileri toplayabilir, saklayabilir, işleyebilir ve aktarabilirler:

* 1. **Saklamaya İlişkin Açıklamalar**

KVKK’nın 3.(üçüncü) maddesinde “*kişisel verilerin işlenmesi”* kavramı tanımlanmış 4.(dördüncü) 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(beş) ve 6.(altıncı) maddelerde ise *“kişisel verilerin işleme şartları”* sayılmıştır.

Buna göre, BSCI iş faaliyetleri çerçevesinde kişisel veriler, *ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.*

* 1. **Saklamayı Gerektiren Hukuki Sebepler**

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

* 6098 Sayılı Türk Borçlar Kanunu
* 6102 Sayılı Türk Ticaret 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
* 6361 Sayılı İş Sağlığı ve Güvenliği Kanunu
* 4857 Sayılı İş Kanunu
* İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik
* Arşiv Hizmetleri Hakkında Yönetmelik
* Tıbbi Cihaz Yönetmeliği
* Tıbbi Cihaz Satış, Reklam ve Tanıtım Yönetmeliği
* Tıbbi Cihaz Klinik Araştırmaları Yönetmeliği
* Vücuda Yerleştirilebilir Aktif Tıbbi Cihazlar Yönetmeliği

Bu kanunlar uyarınca, yürürlükte olan diğer ikincil düzenlemeler ve bununla sınırlı olmamak üzere; BSCI’ın uyması gereken mevzuat ve idari düzenlemeler uyarınca öngörülen saklama süreleri boyunca saklanmakta ve işlenmektedir.

* 1. **Saklamayı Gerektiren İşleme Amaçları**
* **Klinik araştırma ve ruhsatlandırma işleri:** Spesifik olarak, çalışanlar, klinik çalışma denekleri hakkında ve araştırmacılar hakkında Kişisel Veriler toplayabilir, işleyebilir ve aktarabilirler. Çalışanlar, vijilans faaliyetleri ile bağlantılı konularda da Kişisel Veriler toplayabilir, işleyebilir ve aktarabilirler. Bu süreçlerde hastalar hakkında toplanan veriler anonimleştirilmiş olmak zorundadır.
* **Kurumsal iletişimi sağlamak**,
* **Kurum güvenliğini sağlamak,**
* **İstatiksel çalışmalar yapabilmek,**
* **Satış ve pazarlama:** Çalışanlar, müşteri şikayetleri izleme sistemleri yoluyla ve aracılığıyla, ticari müşteriler (örneğin doktorlar, hemşireler, eczacılar, vb.) hakkında Kişisel Verileri aşağıdaki şartlarla toplayabilir, işleyebilir ve aktarabilirler. Çalışanlar, BSCI ürünlerinin tüketicileri hakkında da aşağıdaki şartlara uymak suretiyle Kişisel Veriler toplayabilir, işleyebilir ve aktarabilirler.
* **İnsan kaynakları süreçlerini yürütmek:** Çalışanlar, BSCI çalışanlarının işe alınması, ücretleri, yan hakları ve bağlantılı konulara ilişkin Kişisel Verileri Türkiye’deki mevcut yasalar çerçevesinde toplayabilir, işleyebilir ve aktarabilirler. Çalışanlar, iş başvuruları hakkında da Kişisel Verileri Türkiye’deki mevcut yasalar çerçevesinde toplayabilir, işleyebilir ve aktarabilirler.
* **İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek**
* **Tedarikçiler:** Birlikte çalışılacak, hizmet alınacak herhangi bir şahıs şirketi olması durumunda yetkili gerçek kişinin verileri toplanabilir, işlenebilir ve aktarılabilir.
* **BSCI ile iş ilişkisi bulunan gerçek/tüzel kişilerle irtibat sağlamak,**
* **Yasal raporlamalar yapmak**
* **Çağrı merkezleri ve ürün bildirim süreçlerini yönetmek**
* **İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü**
  1. **İmhayı Gerektiren 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 BSCI tarafından kabul edilmesi,
* BSCI’in, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya KVKK’da öngörülen süre içinde cevap vermemesi hallerinde; Kişisel Verileri Koruma Kurulu’na şikâyette bulunması ve bu talebin Kişisel Verileri Koruma Kurulu 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, BSCI tarafından ilgili kişinin talebi üzerine yahut sürenin bitmesi halinde ilk periyodik imha sürecinde silinir, yok edilir ya da re’sen silinir, yok edilir veya anonim hale getirilir

1. **KAYIT ORTAMLARI**

Kişisel veriler BSCI tarafından Tablo 1’de listelenen ortamlarda hukuka uygun olarak güvenli bir şekilde saklanır.

*Tablo 1: Kişisel veri saklama ortamları*

|  |  |
| --- | --- |
| Elektronik Ortamlar | Elektronik Olmayan Ortamlar |
| Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, Office 365 sistemi, SAP-WINCHL-EBS-UTS sunucuları, one drive, global şikayet sistemi(GCS2), MS Teams, Success Factors, web, dosya paylaşım vb.)  Yazılımlar(ofis yazılımları, VERBİS)  Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)  Kişisel bilgisayarlar(Masaüstü, dizüstü)  Optik diskler (CD, DVD vb.)  Çıkartılabilir bellekler (USB, Hafıza Kart vb.)  Yazıcı, tarayıcı, fotokopi makinesi | Kağıt  Manuel veri kayıt sistemleri(anket formları, ziyaretçi defterleri)  Yazılı, basılı, görsel ortamlar |

1. **KİŞİSEL VERİ İŞLEME KOŞULLARI**
   1. Kişisel Verilerin bu Politikaya uygun olarak işlenebilmesi ve kullanılabilmesi için, Veri Süjesinden Kişisel Verilerinin işlenmesi konusunda izin istenmesi ve Veri Süjesinin açık rızasının alınması gerekir. Bu amaçla çalışanlarımız, hizmet aldığımız hukukçular tarafından, onaylanan onam formlarını ve aydınlatma metinlerini kullanmalıdırlar.
   2. Ancak aşağıda sayılan istisnalardan birinin söz konusu olması halinde Veri Süjesinden açık rıza alma şartı uygulanmaz:
      1. Kişisel Verileri işlemenin, Veri Süjesinin de taraf olduğu bir sözleşmenin ifası ve uygulanması için ya da bir sözleşmeye girmeden önce (örneğin, sponsorluk ücretinin ödenebilmesi için ilgili kişinin ödeme bilgilerinin işlenmesi) gerekli adımları atmak için zorunlu olması halinde.
      2. Kişisel Verileri işlemenin bir kanuni yükümlülüğe uymak için zorunlu olması halinde.
      3. Kişisel Verileri işlemenin bir kamu otoritesinin veya resmi makamın yetkileri dahilindeki bir görevin ifası için gerekli olması halinde.
      4. Kamuya açık olan genel bilgilerin, yoruma dayanan bilgilerin ve/veya istatistik veri ve bilgilerinin işlenmesi halinde.
   3. **Veri Sorumlusu olarak BSCI’in Aydınlatma Yükümlülüğü:**

Veri Sorumlusu olarak, işbu Politika’nın 7.2. maddesinde anıldığı şekilde Kişisel Verilerin işlenebilmesi ve kullanılabilmesi için her zaman Veri Süjesinden açık rıza almamız şart olmasa dahi, her koşulda Veri Süjelerine aşağıdaki konularda bilgi verme yükümlülüğümüz bulunmaktadır.

* 1. Veri sorumlusunun ve varsa temsilcisinin kimliği,
  2. Kişisel verilerin hangi amaçla işleneceği,
  3. İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
  4. Kişisel veri toplamanın yöntemi ve hukuki sebebi,
  5. işbu Politika’nın 9.1. maddesinde sayılan diğer hakları
  6. **Özel Nitelikli Kişisel Verilerin işlenmesinde Uyulacak Kurallar:**

İş kanunları ve mevzuatından doğan belirli hakların kullanılması veya belirli yükümlülüklerin yerine getirilmesi amaçlarıyla gerekli olmadıkça ve Veri Koruma Mevzuatı başta olmak üzere yürürlükteki sair mevzuat gereğince izin ve yetki verilen durumlar haricinde, Özel Nitelikli Kişisel Veriler işlenmeden önce bu verileri işlemek için ilgili kişinin açık izin ve rızasını mutlaka ve daima almak gerekir.

* 1. **Çalışanların Kişisel Verilerinin İşlenmesinde Uyulacak Kurallar:**

Çalışanlara ait Özel Nitelikli Kişisel Veriler de dahil olmak üzere Kişisel Verilerin İş Kanunu ve diğer ilgili mevzuat uyarınca yahut BSCI tarafından belirlenen başka amaçlarla işlenebilmesi için, halihazırda BSCI çalışanı bulunan kişilere İnsan Kaynakları Departmanı tarafından Çalışan Veri Gizliliği Bildirimi’nin imzalatılması ve bu dokümanların departman dahilinde saklanması suretiyle aydınlatma ve açık rıza temini yükümlüğünün yerine getirilmesi ve depolanması gerekmektedir.

Çalışanlara ait kişisel verilerin işlenebilmesi bakımından; hali hazırda çalışan durumunda bulunmayan, işe alım süreci tamamlanacak olan kişilere ilişkin Kişisel Verilerin işlenebilmesinin temini için, ilgili kişiye imzalatılacak olan iş sözleşmesine İnsan Kaynakları Departmanı tarafından İş Sözleşmesine Eklenecek Kişisel Veri Koruma Maddesi’nin eklenmesi ve iş sözleşmesinin bu haliyle imzalanması suretiyle aydınlatma yükümlülüğünün yerine getirilmesi gerekir.

Son olarak Özel Nitelikli Kişisel Veriler de dahil, Kişisel Veri İşleme faaliyetinde bulundan kişilere İnsan Kaynakları Departmanı tarafından Kişisel Veri Gizliliği Taahhütnamesi’ni imzalatılarak bu dokümanların departman dahilinde saklanması gerekir.

* 1. **Müşterilere Ait Kişisel Verilerin Pazarlama Amaçlarıyla İşlenmesi ve Kullanılmasında Uyulacak Kurallar:**

Bir çalışanımızın, müşterilerin Kişisel Verilerini doğrudan pazarlama yapmak amacıyla toplamak ve/veya bu amaçla Kişisel Verileri işlemek istemesi halinde, bu verileri toplamadan yahut başkaca bir şekilde bilgisi dahiline girdiyse bu amaçlarla işlemeye başlamadan önce müşterilerin açık rızasını alması gerekir. Bunun haricinde Veri Süjeleriyle ticari iletişim kurmak için de, bu kişilere istedikleri zaman kendileriyle ticari iletişim kurulmasından vazgeçme imkanları olduğu hatırlatılarak, izin alınması gerekir.

* 1. **Görevi Gereği Kişisel Veri İşleyen Çalışanların Uyması Gereken Kurallar:**

Görevlerinin bir gereği olarak ve görevleri esnasında, BSCI adına Kişisel Verileri işlerken, çalışanlarımızın aşağıda sayılan koşullara uymaları zorunludur:

* + 1. Kişisel Verilerin Veri Koruma Mevzuatı’na uygun bir şekilde, meşru yollarla ve adil bir biçimde işlenmesi gerekir.
    2. Kişisel Verilerin sadece izin verilen ve açıklanan yasal amaçlar için işlenmesi gerekir.
    3. Veri Süjesine açıklamayan veya meşru olmayan bir amaç için kesinlikle veri işlenmemesi ve saklanmaması gereklidir.
    4. Kişisel Verilerin işlenme amacı için yeterli olması, bu amaçla ilişkili ve bağlantılı olması ve işlenme amacına kıyasla aşırı miktarda veya sayıda olmaması gerekir.
    5. Kişisel Verilerin doğru ve gerçek olması ve gerektiğinde güncellenmesi gerekir.
    6. Herhangi bir amaçla işlenen ve kullanılan Kişisel Verilerin bu amaç için gerekli olan süreden daha uzun bir süreyle tutulmaması ve saklanmaması gerekir.
  1. **Görevi Gereği Özel Nitelikli Kişisel Veri İşleyen Çalışanların Uyması Gereken Kurallar:**

Görevlerinin bir gereği olarak ve görevleri esnasında BSCI adına Özel Nitelikli Kişisel Veri işlemekte olan çalışanların işbu Politika’nın 7.7. maddesinde sözü edilmiş olan kurallara uymalarının yanı sıra Kişisel Veri Gizliliği Taahhütnamesi’ni(bkz. madde 7.6) imzalamaları gerekir.

* 1. **Kişisel Verilerin Transferi ve Devri Gerçekleştirirken Uyulması Gereken Kurallar:**
     1. Çalışanlarımız, Veri Koruma Mevzuatı’nın uyarınca belirlenen koşullar haricinde herhangi bir üçüncü kişiye veri transfer etmeyeceklerdir.
     2. Çalışanlarımız, Kişisel Verileri, İlgili Kişi’nin açık rızası bulunmadıkça, Kişisel Verileri Koruma Kurulu tarafından belirlenecek ve ilan edilecek olan ‘Yeterli Korumanın Bulunduğu Ülkeler’ dışında bir ülkeye transfer etmeyeceklerdir.
     3. Kişisel Veriler, bahsi geçen ‘Yeterli Korumanın Bulunduğu Ülkeler’ dışındaki bir ülkeye, ancak ve sadece ilgili Veri Süjesi tarafından bu transfere açık izin ve rızası verildiği takdirde transfer edilebilecektir.
  2. **Tedarikçilerle Sözleşme Yapılırken Uyulması Gereken Kurallar:**
     1. BSCI tarafından tedarikçilerinin yetkililerinin de Kişisel Verileri işlenebilmektedir. Çalışanlar sözü edilen yetkililere ilişkin olarak aydınlatma yükümlülüğünün yerine getirilmesi maksadıyla sözleşme ilişkisine girilecek tedarikçilerine Ek-1 Tedarikçilere Veri Gizliliği Bildirimi göndermelidir.
     2. BSCI olarak tedarikçiler aracılığıyla işlenebilecek Kişisel Verilerin korunması ve hukuka uygun şekilde işlenmesini temin edebilmek için Ek-2’te yer alan Kişisel Veri Koruma Protokolü, tedarikçilerle imzalanacak sözleşmeler sırasında sözleşmeye ek yapılarak imzalanmalıdır.

1. **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 KVK’nın 12. maddesiyle Kanunun 6. maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kişisel Verileri Koruma Kurulu tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde BSCI tarafından teknik ve idari tedbirler alınır.

* 1. **Teknik Tedbirler**

BCSI tarafından kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için kişisel verilerle ilgili olarak aşağıdaki tedbirler alınmıştır:

* Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
* Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
* Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki

matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.

* Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik

önlemleri alınmaktadır.

* Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
* Erişim logları düzenli olarak tutulmaktadır.
* Güncel anti-virüs sistemleri kullanılmaktadır.
* Güvenlik duvarları kullanılmaktadır.
* Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de

sağlanmaktadır.

* Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların

takibi de yapılmaktadır.

* Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
* Saldırı tespit ve önleme sistemleri kullanılmaktadır.
* Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
* Şifreleme yapılmaktadır.
* Veri kaybı önleme yazılımları kullanılmaktadır.
* Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi

sistemleri güncel halde tutulmaktadır.

* Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve

alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

* 1. **İdari Tedbirler**

BSCI 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, ilgili diğer mevzuat hakkında eğitimler verilmektedir.

* Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik

önlemleri alınmaktadır.

* Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık

çalışmaları yapılmaktadır.

* Çalışanlar için yetki matrisi oluşturulmuştur.
* Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal

politikalar hazırlanmış ve uygulamaya başlanmıştır.

* Gerektiğinde veri maskeleme ve anonimleştirme uygulanmaktadır.
* Gizlilik taahhütnameleri yapılmaktadır.
* Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
* İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
* Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
* Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
* Kişisel veri güvenliğinin takibi yapılmaktadır.
* Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri

alınmaktadır.

* Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği

sağlanmaktadır.

* Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
* Kişisel veriler mümkün olduğunca azaltılmaktadır.
* Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların

takibi de yapılmaktadır.

* Mevcut risk ve tehditler belirlenmiştir.
* Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş

ve uygulanmaktadır.

* Kişisel veri işlemeye başlamadan önce BSCI, çalışanları yahut veri işleyenleri

tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.

* Kişisel veri işleme envanteri hazırlanmıştır.
* Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı

sağlanmaktadır.

1. **VERİ SÜJELERİNİN HAKLARI**
   1. Kişisel Verileri işlenen tüm Veri Süjeleri, tarafımıza başvurarak kendisiyle ilgili;
2. Kişisel veri işlenip işlenmediğini öğrenme,
3. Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
4. Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
5. Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
6. Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
7. Veri Koruma Mevzuatı’nda öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
8. (e) ve (f) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
9. İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
10. Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.
    1. Kişisel Verilerin doğrudan, pazarlama çabalarının bir parçası olarak toplandığı durumlarda, Veri Süjesi, kendisine ait Kişisel Verilerin üçüncü şahıslara verilmesine veya pazarlama amaçlarıyla kullanılmasına itiraz etme hakkına ya da Kişisel Verileri üçüncü şahıslara verilmeden veya pazarlama amaçlarıyla kullanılmadan önce durumun kendisine bildirilmesini talep etme hakkına sahiptir.
    2. İlgili kişilerin bu başvurularının, Başvuru Yanıtlama ve Güvenlik Olaylarına Müdahale Politikası içinde anıldığı şekilde yanıtlanması gerekmektedir.
11. **GÜVENLİK KOŞULLARI**
    1. Çalışanlarımız, Kişisel Verileri kazayla veya yasadışı bir şekilde imha olma riskine ya da kazayla kaybolma, tahrif edilme, yetkisiz ifşa veya yetkisiz erişim risklerine(“**Güvenlik Olayı**”) karşı korumak amacıyla, aşağıdakiler de dahil gereken tüm makul güvenlik önlemlerini alırlar:
       1. Kişisel Verilere erişimi sadece görevlerinin ifası esnasında bu bilgilere erişmesi zorunlu olan çalışanlarla sınırlı tutmak.
       2. Uygunsa, şifre korumalı elektronik dosyaları kullanmak.
       3. Kişisel Verileri içeren dosyaları düzenli saklamak ve bu dosyalara fiziksel erişimi gerektiği gibi ve uygun şekilde kısıtlamak.
       4. Kişisel Verilere yetkisiz erişim veya Kişisel Verilerin usulsüz kullanımı gibi olay ve durumlardan haberdar olduğunda bunları derhal âmirine bildirmek.
       5. Kişisel Verileri ilk belirtilen amacı dışında bir amaçla kullanmadan önce ilgili Veri Süjesinden Veri Koruma Mevzuatı uyarınca açık rıza almak ve işleme konusuyla ilgili aydınlatma yükümlülüğünü yerine getirmek.
    2. Kişisel Verileri korumak için alınan güvenlik tedbirlerini periyodik olarak inceleyip değerlendiririz ve böylelikle işlenen Kişisel Verilerin korunması için ilave güvenlik tedbirlerine veya prosedürlerine ihtiyaç olup olmadığını tespit ederiz.
    3. Herhangi bir Güvenlik Olayı’nın oluşması halinde BSCI’in izlemesi gereken adımlarsa “Başvuru Yanıtlama Ve Güvenlik Olaylarına Müdahale Politikası”nda gösterilmiştir.
12. **KİŞİSEL VERİLERİ İMHA TEKNİKLERİ**

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

* 1. **Kişisel Verilerin Silinmesi**

Kişisel veriler Tablo-2’te verilen yöntemlerle silinir.

*Tablo 2: 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 yedekleri ile birlikte 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. |

* 1. **Kişisel Verilerin Yok Edilmesi**

|  |  |
| --- | --- |
| 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. |

* 1. **Kişisel Verilerin Anonim Hale Getirilmesi**

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.

1. **VERİ TÜRLERİNE GÖRE SAKLANMA VE İMHA SÜRELERİ**
   1. Aşağıdaki tabloda belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, bu sürelerin takibinden ve muhafaza süresi dolan verilerin imha edilmesinden Veri Koruma Komitesi sorumludur.
   2. Veri Koruma Komitesi’nin takibinden sorumlu olduğu BSCI periyodik imha süresi 2 yıl olarak belirlenmiştir. Veri Koruma Komitesi bu sürelere uygun olarak imhaların gerçekleştirilmesinden ve muhafaza süresi dolan kişisel verilerin imhasına ilişkin gerekli hatırlatmaları yapmak bakımından görevli ve yetkilidir.

*Tablo 4: Kişisel veri saklama ve imha süreleri*

|  |  |  |
| --- | --- | --- |
| **VERİ TÜRÜ** | **MUHAFAZA SÜRESİ** | **İMHA SÜRESİ** |
| E-postalar ve şirket içi yazışmalar | **10 yıl** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Sözleşmeler | **Sözleşmenin sona ermesini takip eden 10 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Müşteri Kayıtları | **Müşteri ile girilen son etkileşimi takip eden 10 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| SMM Kayıtları | **SMM ile girilen son etkileşimi takip eden 10 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İK Çalışan Kayıtları | **Çalıştıkları süre boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İK Eski Çalışan Kayıtları | **İşten ayrılmalarını takip eden 10 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| İK Çalışan Adaylarına İlişkin Kayıtlar | **Başvuruyu takip eden 2 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Muhasebe ve Finans Kayıtları | **10 yıl** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Şirket İçi Şikayetler ve İlgili Belgeler | **10 yıl** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Ürün güvenliği/kalite/olumsuz olay bildirimleri | **Bildirim tarihinden itibaren 10 yıl boyunca** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Hukuk Kayıtları | **10 yıl** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Resmi Yazışmalar | **Süresiz** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |
| Vergi Kayıtları | **5 yıl** | Saklama süresinin bitimini takip eden ilk periyodik imha süresinde |

1. **KAYIT SİSTEMİ:**

Bu Politikanın orijinal versiyonu, Veri Koruma Komitesi tarafından saklanmakta ve tutulmaktadır.

1. **EKLER:**

Ek-1 Tedarikçilere Veri Gizliliği Bildirimi

Ek-2 Kişisel Veri Koruma Protokolü