

S.S. BURSA ECZACILAR ÜRETİM TEMİN ve DAĞITIM KOOPERATİFİ ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

1. AMAÇ

İşbu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanununun (KVKK) 6. Maddesinde ve Kişisel Verileri Koruma Kurulunun 31/01/2018 tarih, 2018/10 sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemlerin Belirlenmesine Dair Kişisel Verileri Koruma Kurulu Kararında öngörüldüğü üzere özel nitelikli kişisel verilerin işlenmesinde uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlerin belirlenmesi ve uygulanmasına ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.

2. KAPSAM

İşbu Politika, Şirketin çalışanlarını, iş ortaklarını, tedarikçilerini, müşterilerini ve Şirket tarafından özel nitelikli kişisel verisi işlenen tüm gerçek kişileri kapsamaktadır.

İşbu Politika kapsamında;

- Özel nitelikli kişisel verisi işlenen gerçek kişilere,
- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik veya fiziksel ortamlara,
- Özel nitelikli kişisel verilerin işlenmesine ve aktarımına,

ilişkin alınması gereken önlemler ve uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirlere ilişkin süreçler düzenlenmektedir.

3. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ SÜREÇLERİNDE YER ALAN PERSONELE YÖNELİK ÖNLEMLER

a. Personelin Eğitimi ve Farkındalık Çalışmaları

- İşbu Politika'nın uygulanması Kişisel Verileri Koruma Komitesi tarafından sağlanacaktır.
- İşbu Politika ile özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan Şirket çalışanlarının görev tanımları gereği yürüttüğü faaliyetler doğrultusunda, KVKK ve buna bağlı yönetmelikler çerçevesinde, özel nitelikli kişisel veri güvenliği konularına ilişkin düzenli eğitim almaları, tüm Şirket çalışanlarına yönelik farkındalık çalışmaları yapılması sağlanacaktır. Söz konusu bu eğitim ve farkındalık çalışmalarının belirlenmesi ve planlanması doğrultusunda ilgili personele uygun takvimin hazırlanması ve bildiri ile çalışanların eğitimlere katılımlarının kaydının tutulması ve takibinin sağlanması yükümlülükleri Kişisel Verileri Koruma Komitesi tarafından yerine getirilecektir.
- İşbu Politikada tanımlanan faaliyetlere ilişkin ilgili yetki ve sorumluluklar, Şirket uygulamaları, tüm Şirket yazılım ve donanımları, Şirket ağları ve internet erişimi faaliyetlerine ilişkin erişim ve yetkilendirme süreçlerine uygun bir şekilde özel nitelikli kişisel verilere erişim yetkisine sahip çalışanlar tarafından yerine getirilecektir.

b. Rol/Profil Tanımlama

- Şirket faaliyetlerinin yürütülmesi için kullanılan sistemler üzerinde, departmanlara ve ilgili çalışanlara rol/profil tanımlaması yapılacaktır. Bu tanımlar Kişisel Verileri Koruma Komitesi tarafından yapılacak olup, kişisel verilere erişimler rol/profil tanımları çerçevesinde sınırlandırılacaktır. Bu sayede işe yeni başlayan çalışana tanımlanan role/profile göre çalışanın pozisyonunun gerektirdiği tüm yetkiler ve erişimler otomatik olarak hesaba eklenmiş olacaktır.
- Kişisel verilerin işlenmesi ve erişimi faaliyetlerinin, Kişisel Verileri Koruma Komitesi tarafından tanımlanan rol/profil tanımlarına uygun yürütüldüğüne ilişkin denetimler Kişisel Verileri Koruma Komitesi tarafından yapılacaktır. Rol/profil tanımlamalarında herhangi bir değişikliğe ihtiyaç duyulması durumunda gerekli düzenlemeler Kişisel Verileri Koruma Komitesi tarafından gerçekleştirilecektir.

c. Yetki Tanımlama

- Şirket faaliyetlerinin yürütülmesi için kullanılan sistemler üzerinde departmanlara ve ilgili personele Kişisel Verileri Koruma Komitesi tarafından yapılacak rol/profil tanımlamaları ile erişim ve yetki sınırlandırmaları gerçekleştirilecektir.
- Kişisel Verileri Koruma Komitesi tarafından yapılacak olan belirlemeler ve sınırlandırmalar çerçevesinde rol/profillere erişim yetki tanımlamalarının yapılması ve bu tanımlamaların hukuka ve Şirket ihtiyaçlarına uygunluğunun denetlenmesi, güncelliğinin sağlanması ve bunlara ilişkin gerekli düzenlemelerinin yapılması için koordinasyonun sağlanması yükümlülüğü Kişisel Verileri Koruma Komitesinin sorumluluğundadır.

d. Kullanıcı Tanımlama

- Şirket faaliyetlerinin yürütülmesi için kullanılan sistemler üzerinde departmanlara ve çalışanlara ilişkin Kişisel Verileri Koruma Komitesi tarafından yapılacak olan belirlemeler ve sınırlandırmalar çerçevesinde, Kişisel Verileri Koruma Komitesi tarafından çalışanların görev tanımı doğrultusunda kendilerine özgü kullanıcı hesabı açılacak ve ilgili birim tarafından uygun rol/profil atanacaktır.
- Kişisel Verileri Koruma Komitesi, Şirket departmanları ve çalışanlarına tanımlanacak olan rol/profil atanması için belirlenen sınırlamaların ve bu tanımlamaların Kanuna, ikincil mevzuatlara ve Şirket ihtiyaçlarına uygunluğunun ve güncelliğinin denetiminden sorumludur.
- Rol/profil tanımlamalarını gerçekleştiren departman Yöneticileri ile Kişisel Verileri Koruma Komitesi, tanımlanan hesapların Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine göre uygulanıp uygulanmadığını denetlemekle ve herhangi bir ihlal durumunda gerekli disiplin cezalarını belirlemekle sorumludur.
- Çalışan, kendisine tanımlanan hesabı, Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine uygun kullanmakla yükümlüdür.
- Kişisel Verileri Koruma Komitesi tarafından yapılacak olan belirlemeler ve sınırlamalar çerçevesinde görev değişikliği olan ya da işten ayrılan personelin kendisine tahsis edilen envanterin iade alınması, söz konusu iade alma sürecinin denetlenmesi ve gerekli düzenlemelerinin yapılması Kişisel Verileri Koruma Komitesi'ne aittir. Bu durumda envanterin iadesinin sağlanması yükümlülüğü kullanıcıya, envanterin iadesinin hukuka uygun bir şekilde gerçekleşip

gerçekleşmediğini denetleme ve uygulanacak yaptırımları belirleme yükümlülüğü ise kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENDİĞİ MUHAFAZA EDİLDİĞİ VE/VEYA ERİŞİLDİĞİ ORTAMLARA YÖNELİK ÖNLEMLER

a. Elektronik Ortamlar

a.1. Özel Nitelikli Verilerin Kriptografik Yöntemler Kullanılarak Muhafaza Edilmesi

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar veya sistemler kriptografik yöntemlerle şifrelenecektir. Bu veriler bulut ortamına aktarılıyorsa şifrelenerek aktarılacak; söz konusu şifreleme sürecinin devamlılığı, gerekli düzenleme ve güncellemelerin yapılması, şifreleme işleminin hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve uygulanacak yaptırımları belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne ait olacaktır.

Kriptografik anahtarlar;

Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar veya sistemler kriptografik yöntemler kullanılarak şifrelenecek, bu veriler bulut ortamına aktarılıyorsa verilerin şifrelenmesi sonucu oluşturulacak kriptografik/şifreleme anahtarları mümkün olan her yerde ayrı ayrı belirlenecek ve kullanılacaktır. Söz konusu şifreleme sürecinin devamlılığı ile gerekli güncelleme ve düzenlemelerin yapılması, şifreleme işleminin hukuka uygun bir şekilde uygulandığının denetimi ve uygulanacak yaptırımları belirleme yükümlülüğü ilgili departman Yöneticisi ve Kişisel Verileri Koruma Komitesine aittir. Kanunu, ikincil mevzuatları ve işbu Politika hükümlerini ihlal eden çalışanlara uygulanacak disiplin cezaları ilgili departman Yöneticisi ve Kişisel Verileri Koruma Komitesi tarafından belirlenecektir.

Söz konusu kriptografik/şifreleme anahtarlarının güvenli ve farklı ortamlarda tutulmasının belirlenmesi ve kullanılması, söz konusu kriptografik/şifreleme anahtarlarının güvenliğinin sağlanmasının devamlılığının denetlenmesi ve gerekli düzenlemelerinin yapılması, kriptografik/şifreleme anahtarlarının güvenliğinin sağlanmasının hukuka uygun bir şekilde gerçekleşip gerçekleşmediğinin denetlemesi ve uygulanacak yaptırımların belirlenmesi yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

a.2. Log (İz) Kayıtları

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlarda veya sistemlerde özel nitelikli kişisel veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması sağlama, söz konusu loglama işlemlerinin devamlılığının denetlenmesi ve gerekli düzenlemelerinin yapılması, loglama işlemlerinin hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

a.3. Verilerin Bulunduğu Ortamlara Ait Güvenlik Güncellemeleri, Testleri ve Kayıtları

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlara ait güvenlik güncellemelerinin sürekli olarak takip edilmesi, söz konusu güvenlik güncellemelerinin

düzenli olarak takibinin denetlenmesi ve gerekli düzenlemelerin yapılması için koordinasyonun sağlanması, güncelleme işlemlerinin hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlara veya sistemlere ilişkin gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, söz konusu güvenlik testlerinin düzenli olarak yapılması/yaptırılması işlemlerinin sağlanmasının denetlenmesi ve gerekli düzenlemelerinin yapılması için koordinasyonun sağlanması, güvenlik testlerinin düzenli olarak yapılması/yaptırılmasının hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlara ilişkin yapılan tüm güvenlik testlerinin sonuçlarının kayıt altına alınması, söz konusu tüm güvenlik testlerinin sonuçlarının kayıt altına alınması işlemlerinin denetlenmesi ve gerekli düzenlemelerinin yapılması için koordinasyonun sağlanması, tüm güvenlik testlerinin sonuçlarının kayıt altına alınmasının hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını Belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

a.3.1. Verilere Bir Yazılım Aracılığıyla Erişiliyorsa,

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlarda bulunan özel nitelikli kişisel verilere bir yazılım aracılığıyla erişilebiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, söz konusu kullanıcı yetkilendirme işlemlerinin sağlanmasının denetlenmesi ve gerekli düzenlemelerinin yapılması için koordinasyonun sağlanması kullanıcı yetkilendirme işlemlerinin hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını Belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

Özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlarda özel nitelikli kişisel verilere bir yazılım aracılığıyla erişiliyorsa bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, söz konusu güvenlik testlerinin düzenli olarak yapılması/yaptırılması işlemlerinin denetlenmesi ve gerekli düzenlemelerinin yapılması, güvenlik testlerinin düzenli olarak yapılması/yaptırılmasının hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve ihlal durumunda uygulanacak disiplin cezalarını Belirleme yükümlülüğü kullanıcının bağlı bulunduğu departmanın yöneticisi ve Kişisel Verileri Koruma Komitesi'ne aittir.

a.3.2. Verilere Uzaktan Erişim Sağlanıyorsa,

İlgili departman yöneticisi ve Kişisel Verileri Koruma Komitesi, özel nitelikli kişisel verilerin işlendiği muhafaza edildiği ve/veya erişildiği elektronik ortamlarda veya sistemlerde özel nitelikli kişisel verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması, söz konusu kimlik doğrulama sisteminin denetlenmesi ve gerekli düzenlemelerinin yapılması, kimlik doğrulama sisteminin hukuka uygun bir şekilde gerçekleşip gerçekleşmediğini denetleme ve uygulanacak yaptırımları belirlemekle yükümlüdür.

b. Fiziksel Ortamlar

b.1. Özel Nitelikli Kişisel Verilerin Bulunduğu Ortamın Niteliğine Göre Alınacak Güvenlik Önlemleri

İlgili departman Yöneticileri ve Kişisel Verileri Koruma Komitesi, özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği veya erişildiği fiziksel ortamların yangın, su baskını, hırsızlık vb. veri kaybına yol açacak durumlara karşı gerekli tedbirlerin alınmasından, alınan tedbirlerin denetlenmesinden ve gerektiğinde bu tedbirlerde değişiklik yapılmasından ve söz konusu tedbirlerin hukuka uygun şekilde uygulandığına ilişkin denetimin yapılmasından sorumludur.

b.2. Özel Nitelikli Kişisel Verilerin Bulunduğu Ortamların Fiziksel Güvenliğinin Sağlanması

İlgili departman yöneticileri ve Kişisel Verileri Koruma Komitesi özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği veya erişildiği fiziksel ortamlara yetkisiz girişlerin engellenmesi için gerekli güvenlik önlemlerini almakla, alınan bu güvenlik önlemlerinin denetlemekle ve gerektiğinde bu önlemlerde değişiklik yapılmasından ve bu önlemlerin hukuka uygun şekilde uygulandığına ilişkin denetiminden sorumludur.

5. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN AKTARILMASINA YÖNELİK ALINMASI GEREKEN ÖNLEMLER

a. E-posta ile Aktarım

Tüm Şirket çalışanları, özel nitelikli kişisel verilerin e-posta yoluyla aktarıldığı durumlarda, içeriği şifreleyerek, kurumsal e-posta kullanmak suretiyle aktarımı gerçekleştireceklerdir.

İlgili departman Yöneticileri ve Kişisel Verileri Koruma Komitesi, özel nitelikli kişisel verilerin e-posta yolu ile aktarımının, şifreli olarak ve kurumsal e-posta üzerinden gönderildiğini denetlemekle ve herhangi bir ihlal durumunda gerekli disiplin cezalarını belirlemekle sorumludur

b. Harici Hafıza Depolama Ürünleri ile Aktarım

Özel nitelikli kişisel verilerin harici disk, usb, cd vb. taşınabilir ortamlar üzerinden aktarımının yapıldığı durumlarda, içerik kriptografik yöntemlerle şifrelenecektir.

İlgili departman yöneticileri ve Kişisel Verileri Koruma Komitesi, özel nitelikli kişisel verilerin harici disk, usb, cd vb. taşınabilir ortamlar üzerinden aktarımının yapılması durumunda içeriğin şifrenmesini sağlamakla, bu yolla yapılan aktarımların Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine uygunluğunu denetlemekle ve gerekli değişikliklerin yapılmasıyla ve herhangi bir ihlal durumunda gerekli disiplin cezalarını belirlemekle yükümlüdür.

Özel nitelikli kişisel verilerin harici disk, usb, cd vb. taşınabilir ortamlar üzerinden aktarımının yapıldığı durumlarda içeriğin şifrenmesi için kullanılan kriptografik anahtarlar farklı ortamlarda muhafaza edilecektir.

İlgili departman yöneticileri ve Kişisel Verileri Koruma Komitesi, özel nitelikli kişisel verilerin harici disk, usb, cd vb. taşınabilir ortamlar üzerinden aktarımının yapılması durumunda içeriğin şifrenmesi için kullanılan kriptografik anahtarların farklı ortamlarda muhafaza edilmesini sağlamakla, bu kriptografik anahtarların Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine uygun şekilde muhafaza edildiğine ilişkin denetimleri yapmakla ve herhangi bir ihlal durumunda gerekli disiplin cezalarını belirlemekle yükümlüdür.

c. Sunucular Arasındaki Aktarım

Özel nitelikli kişisel verilerin, farklı fiziksel ortamlarda bulunan sunucular arasında aktarımının yapılması durumunda, sunucular arasında VPN veya SFTP kurulması yöntemleriyle veri aktarımı gerçekleştirilecektir.

İlgili departman yöneticileri ve Kişisel Verileri Koruma Komitesi, Özel nitelikli kişisel verilerin, farklı fiziksel ortamlarda bulunan sunucular arasında aktarımının yapılması durumunda, sunucular arasında VPN veya SFTP kurulması yöntemleriyle veri aktarımının gerçekleştirilmesini sağlamakla, bu aktarımın Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine uygun şekilde yapıldığını denetlemekle ve gerektiğinde değişiklikler yapmakla ve ihlal durumunda gerekli disiplin cezalarını belirlemekle yükümlüdür.

d. Kâğıt Ortamı Yoluyla Aktarım

Özel nitelikli kişisel verilerin kağıt vb. evrak üzerinde aktarımının yapıldığı durumlarda, özel nitelikli kişisel veri içeren evrakların kaybolması, fiziken tahrip olması, yetkisiz kişiler tarafından görülmesini engellemek amacıyla gerekli güvenlik önlemlerinin alınması gerekmektedir. Ayrıca bu tür evraklar üzerinde "Özel Nitelikli Veri İçerir" veya "Gizli Belge" ibaresi taşıyan formlar içerisine konularak aktarılacaktır.

İlgili departman yöneticileri ve Kişisel Verileri Koruma Komitesi, Özel nitelikli kişisel verilerin kağıt vb. evrak üzerinde aktarımının yapıldığı durumlarda, özel nitelikli kişisel veri içeren evrakların kaybolması, fiziken tahrip olması, yetkisiz kişiler tarafından görülmesini engellemek amacıyla gerekli güvenlik önlemlerinin alınmasını sağlamakla, bu tür aktarımların Kanuna, ikincil mevzuatlara ve işbu Politika hükümlerine uygun şekilde yapıldığını denetlemekle ve ihlal durumunda gerekli disiplin cezalarını belirlemekle yükümlüdür.

6. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASINDA YAPILACAK GÜNCELLEMELER

Kooperatif, KVK Kanunu'nda yapılan değişiklikler nedeniyle, KVK Kurumu kararları uyarınca ya da ortaya çıkacak gelişmeler doğrultusunda, Özel Nitelikli Kişisel Verilerin Korunması Ve İşlenmesi Politikasında değişiklik yapma hakkını saklı tutmaktadır.

İşbu Özel Nitelikli Kişisel Verilerin Korunması Ve İşlenmesi Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

7. YÜRÜRLÜK

İşbu Özel Nitelikli Kişisel Verilerin Korunması Ve İşlenmesi Politikasında, **04.10.2022** tarihinde ortak klasörde paylaşılarak yürürlüğe girmiştir.

DÖKÜMAN GÜNCELLEME TABLOSU				
Politika Maddesi	Politika Alt Maddesi	Versiyon	Yayın Tarihi	Değişikliğin Tanımı
		1.0	04.10.2022	Kişisel Verilerin Saklanması ve İmhasına İlişkin Politika

