ETİ SODA A.Ş.
ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

Eti Soda A.Ş.
Özel Nitelikli Kişisel Verilerin Korunması Politikası

İÇİNDEKİLER

Eti Soda A.Ş.
Özel Nitelikli Kişisel Verilerin Korunması Politikası

1. POLİTİKA'NIN HAZIRLANMA AMACI

6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" ya da "Kanun") ve Özel Nitelikli Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler konulu Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarih ve 2018/10 sayılı Kararı doğrultusunda işbu **"Özel Nitelikli Kişisel Verilerin Korunması Politikası"(ÖNVP)** şirketimiz nezdinde yürürlüğe girmiştir.

2. KAPSAM

ÖNVP ile 6698 sayılı Kişisel Verilerin Korunması Kanunu (**Kanun/KVKK**) ve ilgili diğer mevzuat kapsamında elde edilen kişisel verilerin gizliliği ve güvenliğinin öneminin farkındalığıyla ilgili mevzuata uyum için gerekliliklerin layıkıyla yerine getirilmesi ve uluslararası standartlarda bir veri koruma ve işleme politikası oluşturulmasını hedeflenmektedir.

Özel nitelikli verilere ilişkin olarak Kanunun 6. maddesi aşağıdaki gibidir:

(1) 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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan 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, tıbbi 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.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

ÖNVP ile şirketimiz tarafından özel nitelikli kişisel verilerin korunması ve işlenmesinde benimsenen esaslar hukuka uygunluk, dürüstlük ve açıklık ilkeleri doğrultusunda ortaya konulmaktadır. Şirketimiz nezdinde özel nitelikli verilerin güvenliğini ve bu verilerin işlendiği mecralara erişimi yetkilendirmesini takip etmek amacıyla **Erişim Yetkilendirme Matrisi** hazırlanmıştır.

3. TANIMLAR

Anonim Hale Getirme	:	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi
Açık Rıza	:	Kişisel verisi işlenecek kişinin ilgili işlem gerçekleştirilmeden önce aydınlatılmasından sonra işlemin yapılmasına rıza beyanında bulunması.
Aydınlatma Metni	:	Kişisel verinin hangi amaçla ne kadar süre saklanacağı, hangi yöntemle toplandığı, nasıl muhafaza edildiği ve 3. kişilerle paylaşılıp paylaşılmayacağı hususlarında ilgili kişiye yapılan açıklama
Başkanlık	:	Kişisel Verilerin Korunması Kurumu Başkanlığı

Envanter	:	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter
İlgili Kişi	:	Kişisel verisi işlenen gerçek kişi
İmha	:	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
İşleme	:	KVKK'nın 3. maddesinde kişisel verilerin kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması işlemleri
Kanun/KVKK	:	Kişisel Verilerin Korunması Kanunu
Kişisel Veri	:	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Örneğin; ad-soyadı, TCKN, e-posta, adres, doğum tarihi, banka hesap numarası vb. dolayısıyla tüzel kişilere ilişkin bilgilerin işlenmesi KVKK kapsamında değildir.
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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kurul	:	Kişisel Verilerin Korunması Kurulu
Kurum	:	Kişisel Verilerin Korunması Kurumu
Özel Nitelikli Hassas Veri	:	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler
VERBİS	:	Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemi
Veri İşleyen	:	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
Veri Sorumluları Sicili	:	Başkanlık tarafından tutulan Veri Sorumluları Sicili
Veri Sorumlusu İrtibat Kişisi	:	Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından sicile kayıt esnasında bildirilen gerçek kişi
Silme	:	Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi
Yok Etme	:	Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi

4. ÖZEL NİTELİKLİ KİŞİSEL VERİSİ ELDE EDİLEN İLGİLİ KİŞİLER

Şirketimiz tarafından özel nitelikli kişisel verisi elde edilen ve işlenen İlgili Kişilere ilişkin tablo aşağıda yer almakta olup; İşbu Politika'nın uygulama alanı ve kapsamı bu tabloda yer verilen ilgili kişilerle sınırlıdır. Bu tanımlamalar dışında yer alan ilgili kişilerin talepleri de şirketimiz tarafından KVKK ve ilgili mevzuat kapsamında işlem yapılacaktır.

Çalışan	:	Adli Sicil Belgesi, Sağlık Verileri, Biyometrik Veri(Parmak İzi)
Çalışan Adayı	:	Sağlık Verisi
Stajyer	:	Sağlık Verileri, Biyometrik Veri(Parmak İzi)
Stajyer Adayı	:	Sağlık Verileri
Bağımsız Yönetim Kurulu Üyesi	:	Adli Sicil Belgesi
Denetim Kurulu Üyesi	:	Adli Sicil Belgesi
Ziyaretçi	:	Sağlık Verisi (Ateş Ölçümü)
Tedarikçi Çalışanı	:	Sağlık Raporu

5. UYGULANAN KRİPTOGRAFİ/ŞİFRELEME YÖNTEMİ

ÖNVP'de yer alan maskeleme tanımlarından; okunabilir durumdaki sayısal verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümü olarak anlaşılacaktır.

Kriptografi için matematiksel yöntemler (algoritmalar) kullanılır ve önemli bilgilerin güvenliği için gerekli gizlilik, aslıyla aynılık, kimlik denetimi ve aslının reddini önleme gibi işlevleri sağlamak amaçlanır. Bu yöntemler, bir bilginin iletimi sırasında ve saklanma süresinde karşılaşılabilecek aktif saldırı ya da pasif algılamalardan bilgiyi dolayısıyla bilginin göndericisi, alıcısı, taşıyıcısı, konu edindiği kişiler ve başka her türlü taraf olabilecek kişilerin çıkarlarını da koruma amacı güderler. Yasal saklama süresi dolan veya geçerlilik süresi tamamlanan veri, SAP yazılımı üzerinde maskelenir. Sabit disk, manyetik bant vb ortamlarda bulunan veriye maskeleme işlemi uygulanmaz. Bu ortamlarda bulunan verilerin güvenliği modüler bazda verilen yetkiler ile sağlanır. Ayrıca veri iki uç arasında paylaşılırken, iletimin gizliliğinin sağlanması için de VPN veya SFTP kullanılmaktadır. Şifrelemenin güvenliği sayısal anahtarın korunmasına bağlı olduğundan bu hususta azami özen gösterilmektedir. Bu yüzden şifreleme için kullanılan anahtarlar, kamuya açık ortamlar üzerinde bulundurulmamakta ve paylaşılmamaktadır.

6. ÖZEL NİTELİKLİ VERİLERİN İŞLENMESİNE İLİŞKİN TEDBİRLER

Özel nitelikli kişisel verilerin bulunduğu fiziksel ve dijital ortamlara sadece **Erişim Yetkilendirme Matrisi**'nde yetkilendirilmiş unvan sahipleri tarafından erişim sağlanmaktadır.

Kişisel veri içeren ve özellikle özel nitelikli veri ihtiva eden belge ve dosyalar "Kişisel Veri İçerir. Gizlidir." ibareli kaşe kullanmak suretiyle kaşelenmekte ve şirketimiz bünyesinde yetkisiz erişimlerin görevliler nezdinde bir farkındalık yaratarak engellenmesi hedeflenmektedir.

Görevlilerin yetki değişikliği olması ve/veya işten ayrılması durumunda sisteme yetkisiz erişimin engellenmesi amacıyla gerekli kontroller gerçekleştirilir, görev değişikliği olan veya sözleşme ilişkisi ortadan kalkan görevlilerin yetki ve erişimi derhal ortadan kaldırılır.

6.1. Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmektedir. Şirketimiz bünyesindeki özel nitelikli veri işleyen veya veri erişimine yetkili olan görevliler KVKK düzenlemeleri ile özel nitelikli veri güvenliği konularında eğitim alır ve azami seviyede farkındalığa ulaşırlar.

6.2. Gizlilik sözleşmeleri yapılmaktadır. Görevliler ile imzalanan sözleşmelere KVKK hükümlerini ihtiva eden bir madde eklenmiş olmakla birlikte kişisel veri işleme süreçlerinde iş görme borcunu yerine getiren görevlilerden Gizlilik Taahhüdü de alınmaktadır.

6.3. Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamları ve süreleri net olarak tanımlanmaktadır. Verilere erişim yetkisine sahip kullanıcıların veri erişim ve işleme yetkileri birbirinden ayrılmış ve görevlinin en üst amirinin onayı ile (aksi bir durum gelişmedikçe) görev süresi boyunca verilen haklara sahip bulunmaktadır. Erişim Yetkilendirme Matrisinde unvan bazlı olarak 3 tip yetkilendirme yapılmıştır. Bunlar; Görüntüleme, Görüntüleme - Düzenleme ve Görüntüleme - Düzenleme - Silme olarak kategorize edilmiştir.

6.4. Periyodik olarak yetki kontrolleri gerçekleştirilmektedir. Dijital ortamdaki bilgiye erişim her kullanıcı için oluşturulmuş kullanıcı kimlikleri ile yönetilmekte ve takip edilmektedir. Bu kimlikler görevlinin şirketimiz adına görev yapmasının sona ermesi üzerine erişime ve kullanıma kapatılır.

6.5. Görev değişikliği olan görevlilerin bu alandaki yetkileri derhal kaldırılmaktadır.

6.5.1 Uygulanacak standart adımlar aşağıda listelenmiştir.

a. **Eski PC'deki Verilerin Taşınması:** Veriler lokal Pc'de data tutulmuyor. İlgili departman dataları file üzerinde tutuluyor. İlgili görevlinin görev veya lokasyon değiştirmesi durumunda erişim yetkileri değiştiriliyor.

b. **Yeni Bilgisayardaki Kullanıcı Ayarları (İsim değiştirme/Disable etme) :** Kullanıcıya yeni bilgisayar verilmesi durumunda mevcut yetki tanımları yapılır. Active domain yapısı kullanıldığı için tanımlamalar otomatik olarak bilgisayara aktarılır.

c. **Guruba Özel Yazılım Yetki Kontrolleri:** Yetki kontrolleri kullanılan programın admin paneli üzerinden yönetilir. Görevlinin görevinin sona ermesi durumunda ilgili hesap silinir.

d. **Zimmetli Eşya Ekipman İade ve Sicil İşlemleri:** Görevi sona eren görevli öncelikle zimmet kaydı olan donanım ve diğer malzemeleri "İlişik Kesme Formu" ile birlikte teslim eder.

6.5.2 Görevi sona eren görevlinin giriş kartları teslim alınmaktadır.

6.5.3 Görevliler, yükleniciler ve dış taraf kullanıcılarla iş ilişkisinin sonlandırılması söz konusu olduğunda; devam eden güvenlik gereksinimleri, yasal sorumluluklar, varsa gizlilik anlaşmalarında tanımlanan sorumluluklar, görev süresinin sonlanmasından sonra da belli bir süre devam edecek olan koşullar bildirilir.

6.5.4 Bu kontrollerin yapılabilmesi için yürürlüğe **İlişik Kesme Formu** uygulamaya alınmıştır.

7. ÖZEL NİTELİKLİ VERİLERİN MUHAFAZA EDİLDİĞİ ORTAMA YÖNELİK TEDBİRLER

Şirketimizde özel nitelikli veriler fiziksel ve elektronik ortamda tutulmaktadır. Bu veriler güvenli şifreleme yöntemleriyle muhafaza edilmekte, şifreler ve anahtarlar güvende ve farklı ortamda tutulmaktadır. Bu ortamlara ait güvenlik sistemleri mevcut olup, güncellemeleri Bilgi İşlem birimimiz tarafından düzenli olarak yapılmaktadır. Özel nitelikli verilerin muhafaza edildiği fiziksel ortamda ise yeterli güvenlik tedbirleri alınmış olup, giriş çıkışa yetkili kişiler belirlenmiştir.

7.1. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği ve/veya Erişildiği Elektronik Ortamlarda Alınan Tedbirlere aşağıda yer verilmektedir.

a) **Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi:** Yazılımlarımız kriptografik veri saklama yeteneğine sahip değildir. Fakat uygulama modüler haklara bölünmüş kullanıcı erişim kimlik/parola yapısı ile yönetilmektedir.

b) **Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulmaktadır.** Sayısal veri, bir sayısal saklama ortamında (Yazılım bazında “SAP”), veriyi içeren dosyanın veya bir veri tabanındaki kaydın şifrelenmesi ile korunmaktadır. Ayrıca veri iki uç arasında paylaşılırken, iletimin gizliliğinin sağlanması için de firewall ve Sftp bazında şifreleme kullanılmaktadır. Şifreleme tipik olarak bir şifreleme algoritması ve algoritma ile kullanılan sadece veriye ulaşmaya yetkili kişilerin erişebildiği bir sayısal anahtar ile sağlanmaktadır. Şifrelemenin güvenliği sayısal anahtarın korunmasına bağlıdır. Bu yüzden şifreleme için kullanılan anahtarlar, kamuya açık ortamlar üzerinde bulundurulmamaktadır ve paylaşılmamaktadır.

c) **Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanmaktadır.**

d) **Verilerin bulunduğu ortamlara ait güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testleri düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır.** Verilerin bulunduğu sistemlere ait işletim sistemi güncellenmeleri düzenli ve kontrollü olarak gerçekleştirilmektedir.

e) **Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılmakta, bu yazılımların güvenlik testlerinin düzenli olarak yapılmakta/yaptırılmakta, test sonuçları kayıt altına alınmaktadır.** Yetkilendirmeler uygulama seviyesinde yapılmaktadır. Uygulamalar Active Directory ile entegre olarak, yetkilendirme buradaki bilgiler kullanılarak yapılmaktadırlar. Yetkilendirme matrisi alınmış ve kontrol edilmiştir. Kullanıcılar mevzuat gereği hakları bulunan bilgileri görmektedirler.

f) **Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi sağlanmaktadır.** Dışarıdan/uzaktan erişim için güvenli VPN tanımlaması yapılmıştır.

7.2. Özel Nitelikli Kişisel Verilerin İşlendiği, Muhafaza Edildiği Ve/Veya Erişildiği Fiziksel Ortamlarda Alınan Tedbirlere aşağıda yer verilmektedir.

a. **Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması için gerekli tedbirler alınmaktadır.** Fiziki ortamda yer alan özel nitelikli kişisel veriler dosyalar halinde İnsan Kaynakları ofis ve arşiv alanları ile İş Sağlığı ve Güvenliği Uzmanı ve İşyeri Hekimi odalarında bulunan

kilitli dolaplarda bulundurulmaktadır. Ofis ve arşiv ortamları yangın duman detektörleri, söndürme sistemleri, alarm ve ikaz sistemleri ile korunmakta ve güvence altında bulundurulmaktadır.

b. **Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışlar engellenmektedir.** Özel nitelikli kişisel verilerin bulunduğu ofis ve arşiv alanları mesai saatleri dışında kilitlenmektedir.

8. ÖZEL NİTELİKLİ VERİLERİN AKTARILMASINA YÖNELİK İLKELER

Şirketimiz özel nitelikli verilerin aktarımında aşağıda yer verilen ilkeleri yerine getirir.

a. Özel Nitelikli Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılır.

b. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla özel nitelikli kişisel veri aktarılmamakta ve taşınabilir harici ortamlarda saklanmamaktadır.

c. Farklı fiziksel ortamlardaki sunucular arasında aktarım gerçekleşiyorsa sunucular arasında VPN veya sFTP yöntemiyle aktarım gerçekleştirilir.

d. Verilerin fiziksel ortamda aktarımı gerçekleşiyorsa evrakların çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmemesi için azami özen gösterilmekte, veriler kapalı zarf içinde üzeri kaşelenerek aktarılmaktadır.

9. YÜRÜTME

ÖNVP hükümlerinin güncellenmesinden aktif olarak süreçlerin denetlenmesinden, veri güvenliği ilkelerinin Şirketimiz nezdinde farkındalığının artırılmasından ve uygulamasından şirketimiz sorumludur.

GENEL MÜDÜR