SAKLAMA VE İMHA POLİTİKASI

6698 sayılı Kişisel Verilerin İşlenmesi Kanunu ‘’KVKK’’ M.11 kapsamında kişisel verileriniz silinir, yok edilir veya anonim hale getirilir. Bununla birlikte ONNOWELL Gıda Kozmetik İç ve Dış Ticaret A.Ş. “ ONNOWELL”, ilgili kişinin talebi üzerine veya veri işleme sebebinin veri sorumlusu ONNOWELL bakımından ortadan kalkması halinde kişisel verilerinizi Kişisel Verileri Koruma Kurulu’nun yayınladığı kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi uyarınca yok eder, siler veya anonim hale getirir. Bu kapsamda işbu ‘’ Saklama ve İmha Politikası’’, rehber uyarınca yerine getirdiğimiz süreçlere ilişkin bilgi amaçlı hazırlanmıştır.

A. Saklamayı Gerektiren Hukuki Sebepler

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

· 6698 sayılı Kişisel Verilerin Korunması Kanunu,

· 6098 sayılı Türk Borçlar Kanunu,

· 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

· 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,

· 4857 sayılı İş Kanunu,

· 5434 sayılı Emekli Sağlığı Kanunu,

· 2828 sayılı Sosyal Hizmetler Kanunu

· İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

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

B. Saklamayı Gerektiren İşleme Amaçları

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

İnsan kaynakları süreçlerini yürütmek.

İletişim faaliyetlerinin yürütülmesi.

Mal, hizmet, üretim ve operasyon süreçlerinin yürütülmesi.

Müşteri ilişkileri yönetim süreçlerinin yönetilmesi.

Pazarlama ve analiz çalışmalarının yürütülmesi.

Sözleşme süreçlerinin yürütülmesi.

Ürün ve hizmetlerin pazarlama süreçlerinin yürütülmesi.

Finans ve muhasebe işlerinin yürütülmesi.

Reklam kampanya promosyon süreçlerinin yürütülmesi.

İade ödeme işlemi yapılabilmesi

Online satış faaliyetlerinin yürütülmesi

Bilgi Güvenliği Süreçleri Yürütülmesi

Müşteri ilişkileri yönetim süreçlerinin yönetilmesi.

Müşteri memnuniyetine yönelik aktivitelerin yürütülmesi.

Talep ve şikayetlerin takibi

Mal/Hizmet Satış sonrası destek hizmetlerinin yürütülmesi

Şirket iletişimi sağlamak.

Şirketin güvenliğini sağlamak,

İstatistiksel çalışmalar yapabilmek.

İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.

Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.

Şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.

Yasal raporlamalar yapmak.

Çağrı merkezi süreçlerini yönetmek.

İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

C. 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 Kanunun 12 nci maddesiyle Kanunun 6 ncı maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için kurul tarafından ilan edilen yeterli önlemler çerçevesinde Şirket tarafından teknik ve idari tedbirler alınır.

C.1. Teknik Tedbirler

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

· Sızma (Penetrasyon) testleri ile şirketimiz 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.

· Şirketimizin 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.

· Şirket 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.

· Şirket, 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 Kurula bildirmek için şirket 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.

· Şirket internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.

· Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

· Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.

· Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

· Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

· Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

C.2 İdari Tedbirler

Şirket 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.

·Şirket tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.

· Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.

· Kişisel veri işlemeye başlamadan önce Şirket tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.

· Kişisel veri işleme envanteri hazırlanmıştır.

· Şirket içi periyodik ve rastgele denetimler yapılmaktadır.

· Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

D.KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

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

D.1 Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-1'de verilen yöntemlerle silinir.

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.

D2. Kişisel Verilerin Yok Edilmesi

Kişisel veriler, Kurum tarafından Tablo-2'de verilen yöntemlerle yok edilir.

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.

D.3. 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.

E.Kişisel Verilerin Saklanma Süreleri

SAKLAMA SÜRELERİ

İLGİLİ KİŞİ VERİ KATEGORİSİ SAKLAMA SÜRESİ

Çalışan Özlük Dosyası, İş Sözleşmesi, SGK'ya bildirilen maaş bildirimleri İşten ayrılıştan itibaren 15 yıl

Çalışan İş sözleşmesi, özlük ve SGK'ya bildirilen ödemeler haricindeki kişisel veriler İş Sözleşmesinin bitimin takip eden yıldan itibaren 10 yıl

Çalışan İşyeri kişisel sağlık dosyasına ilişkin veriler Hizmet sözleşmesinin bitiminden itibaren 30 yıl

Çalışan Video Kamera Görüntüleri Kayıttan itibaren 2 yıl

Tedarikçiler ,Çözüm Ortakları, Danışmanlar Kimlik bilgileri, iletişim bilgileri ,finansal bilgileri Ticari ilişkinin sona ermesinden itibaren TBK 146 ve TTK 82 maddeleri uyarınca 10 Yıl

Tedarikçiler ,Çözüm Ortakları, Danışmanlar Video kamera kaydı, telefon görüşmeleri ses kaydı Verinin elde edilmesinden itibaren 2 yıl

Ziyaretçi İsim, soyisim, T.C. Kimlik Numarası, Pasaport numarası, şirket bina girişlerinde sürücü ehliyeti,plaka, telefon görüşmeleri ses kaydı, IP bilgisi Verilerin elde edilmesinden itibaren 2 yıl

Aday çalışan İş başvuru bilgisi ve iş başvuru formu Bu veri cv güncelliğine yitirene kadar ve en fazla elde edilmesinden itibaren 2 yıla kadar

Aday çalışan Video kamera kaydı, telefon görüşmeleri ses kaydı Verinin elde edilmesinden itibaren 2 yıl

Müşteri İsim, soyadı, T.C kimlik numarası, iletişim bilgisi, ödeme bilgisi ve araçları, 5651 sayılı kanundan kaynaklanan IP erişim bilgisi Her bir ürünün teslim tarihinden itibaren TBK 146 ve TTK 82 maddeleri uyarınca 10 Yıl

MüşteriSes kaydı , Görsel Kayıtlar Verinin elde edilmesinden itibaren 2 yıl

Veri İmha Süreci

Şirket, kişisel verilerin korunması ve işlenmesine ilişkin politika, kişisel veri saklama ve imha politikası, ilişkili yasalar ve Kişisel Verilerin Korunması Kanunu uyarınca ilgili kişisel veriye ilişkin silme, anonimleştirme, yok etmeye ilişkin yükümlülüğün doğmasından itibaren 6 ay içinde söz konusu verileri siler, anonim hale getirir, yok eder.

İlgili kişi, kendisine ait kişisel verilerin silinmesini, yok edilmesini Kanunun 13'üncü maddesi uyarınca şirketten talepte bulunarak isteyebilir:

Kişisel veri işleme şartlarının tamamının ortadan kalkması halinde, kişisel verinin silinmesi, yok edilmesi talebinin kendine ulaşmasından itibaren 30 gün içinde ilgili kişinin talebine uygun olarak şirket ilgili kişisel veriyi yok eder, anonim hale getirir, siler.

İlgili kişi silme, anonimleştirme, yok etmeye ilişkin talebini www.onnowell.com'da bulunan veri sorumlusuna başvuru formunu doldurup belirtilen yollarla veri sorumlusuna gönderdiğinde talep alınmış sayılır. Şirket talebe ilişkin ilgili kişiyi bilgilendirir.

Kişisel veriyi işlemeye ilişkin tüm koşulların ortadan kalkmaması halinde, şirket ilgili kişinin talebini reddedebilir. Kanunun 13'üncü maddesiyle uyumlu olarak şirket, talebin reddine ilişkin sebepleri belirterek cevabını talebin alım tarihinden itibaren 30 gün içinde yazılı olarak veya elektronik yolla ilgili kişiyi bilgilendirir.

PERİYODİK İMHA SÜRESİ

Kişisel veri işleme şartlarının tamamının ortadan kalkması halinde periyodik imha süresi şirket tarafından 6 ay olarak belirlenmiştir. Buna göre şirkette her yıl Haziran ve Aralıkaylarında periyodik imha gerçekleştirilir.