VERİ KORUMA ETKİ DEĞERLENDİRMESİ USUL VE ESASLARI HAKKINDA YÖNETMELİK

KVKK_Y3 VERSİYON 1.00

KARDELEN BOYA VE KİMYA SANAYİ TİCARET LİMİTED ŞİRKETİ

VERİ KORUMA ETKİ DEĞERLENDİRMESİ (VKED/DPIA) USUL VE ESASLARI HAKKINDA YÖNETMELİK

1. GİRİŞ ve KAPSAM

1.1. İşbu Veri Koruma Etki Değerlendirmesi (VKED/DPIA) Usul ve Esasları Hakkında Yönetmelik(bundan böyle Yönetmelik olarak anılacaktır) Şirketimizin Bilgi Güvenliği Politikası, Kişisel Verilerin Korunması Politikası ve Çerçeve Politikası ile birlikte değerlendirilmelidir.

1.2. İşbu Yönetmelik, bilgi ve iletişim teknolojileri metodolojisi ya da genel ticari kullanım açısından özellikle yeni teknolojiler kullanıldığında ve veri işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, Şirketimiz veri sorumlusu sıfatıyla, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin değerlendirme yapmak durumunda olduğu zaman (GDPR Md. 35) ya da Bilgi Varlıkları Sahiplerinin kontrol ettikleri bilgi varlıklarına ilişkin yıllık gözden geçirme süreçlerinde Veri Koruma Etki Değerlendirmesi yaparken takip edilmesi gereken usul ve esasları düzenlemektedir.

1.3. Tanımlar: İşbu yönetmelik açısından Bilgi Varlığı: kardelen Boyanın sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu varlıklardır.

1.4. Bilgi Varlığının Sahibi: İlgili varlığın kullanıldığı iş alanının yöneticisidir

2. VERİ KORUMA ETKİ DEĞERLENDİRMESİ

2.1. Bilgi Varlığının Sahibi olarak atanan çalışanların Çerçeve Politikada açıklanan sorumlulukları doğrultusunda kontrolleri altındaki bilgi varlıklarını idare etmekle sorumludurlar.

2.2. Bilgi Varlıkları Sahipleri en azından yılda bir kez ve özellikle bilgi varlığında, varlığın muhafaza ve işlenme metotlarında belirgin değişiklikler olması ya da bilgi varlıkları bünyesinde muhafaza edilen kişisel veriler üzerinde değişiklikler ön gören yasal düzenleme ya da politika değişiklikleri söz konusu olduğunda ise kesinlikle değişiklikler uygulamaya geçilmeden evvel bir etki değerlendirmesi yapmaları gerekmektedir.

2.3. Bilgi Varlıkları Sahipleri kontrol ettikleri varlıkların güvenliklerinin Şirketin Bilgi Güvenliği Politikasında zikredilen aşağıdaki koşulları karşıladığından emin olmaları gerekir:

- Tüm kullanıcıların bilgiye erişim sağlamadan önce uygun şekilde yetkilendirilmiş olmalıdırlar.
- Bilgi varlığının değer ve/veya hassasiyet değeri ile uyumlu olan makul güvenlik düzeyi sağlanmalıdır.

- Kullanıcılar veri güvenliği ihlali ile sonuçlanan ya da sonuçlanması muhtemel her olayı Veri Koruma İrtibat Görevlisi ve IT Sorumlusuna bildirmelidir. İlgili kullanıcılar IT Destek Ekibini ya da bağlı oldukları Departman Şeflerini ya da Şirket Üst Yöneticilerini ihlal hakkında gecikmeden bilgilendirmelidir.

- Kullanıcılar bilgi varlıkları envanterinin yıllık gözden geçirilmesi kapsamında sahip oldukları varlıklara ilişkin Veri Koruma Etki Değerlendirmesi yapmakla mükelleftir.

2.3.1. Her bir Bilgi Varlığı Sahibi sahip olduğu bilgi varlığı nezdinde tutulan her türlü materyalin aşağıda listelenen şartları her zaman karşılamasını temin etmek için gerekli makul çabayı sarf etmekle mükelleftir:

- Tutulan veriler hukuka uygun olmalıdır.

- Şirketin Bilgi Güvenliği Politikasının 11. Bölümünde zikredilen IT Kaynaklarının Kullanım Koşulları ile uyumlu hareket edilmelidir.

- Tutulan veriler yasadışı materyallere bağlantı sağlayan linkler içermemeli ve Şirketin Bilgi ve Haberleşme Araçlarının Kullanım Koşulları ile uyumsuz içerik barındırmamalıdır.

- İlgili Departman Şefi tarafından onaylanmadığı sürece Şirket namına herhangi bir ticari mal, ürün ya da hizmet tanıtımı ya da bunlarla ilgili yorumlara yer verilmemelidir.

- İlgili Departman Şefi tarafından onaylanmadığı sürece Bilgi Varlığı Sahibinin veya başka herhangi bir kişinin herhangi bir şirketi, ortaklığı, konsorsiyumu veya danışmanlığını veya "özel" faaliyetlerini tanıtma veya yorum içerikli bilgi ve/veya veriler barındırılmamalıdır.

2.3.2. Şirketin bilgi varlıkları bünyesinde yer alıp herhangi bir kişiye ait olan bilgi ve veriler:

- Şirkete ait marka, logo, antetli kâğıt vb.ni ihtiva etmemelidir.

- Muhafaza edilen materyaller Bilgi Varlığı Sahibinin Şirketin IT varlıklarını kullanım noktasındaki yetkilendirme sebebine doğrudan bağlı ya da ilgili olmalıdır.

- İlgili şirket politika ve yönetmelikleri ve bireysel olarak sahip olunan bilgilerin sunuş biçimi, her ne şekilde atıfta bulunulursa bulunulsun, herhangi bir şekilde Şirket'in bireysel olarak sahip olunan bilgilerin kendisi veya içerdiği herhangi bir materyal veya görüş için herhangi bir sorumluluk aldığını veya bunları onayladığı şeklinde yorumlanamaz.

Bireysel olarak sahip olunan tüm bilgilerde, bu bilgilerin Şirket tarafından resmi olarak yayınlanmadığını gösteren onaylanmış bir sorumluluk reddi beyanı ekranda görünmelidir.

2.4. Tüm personel, Şirket tarafından tutulan bilgilerin hangi formatta tutulduğuna bakılmaksızın uygun şekilde korunmasını sağlamak için en iyi bilgi güvenliği uygulamalarını takip etmekten sorumludur. Tüm Departman Şefleri, yönetim sorumluluklarının bir parçası olarak, kendi bölümlerindeki bilgi güvenliği uygulamalarını denetlemekle sorumludur. Bu sürecin bir parçası olarak, Departman Şefleri, departmanları nezdinde tutulan varlıkları gözden geçirecek ve Şirket'in Bilgi Varlık Envanterinin tüm yönetilen varlıkların doğru bir şekilde yansıttığını teyit etmek için gerekli tedbir ve kontrolleri sağlamakla mükelleftirler.

2.5. Bilgi Varlıkları Envanteri, bilgi ve haberleşme teknolojileri güvenliği ve IT varlıklarının yönetimi noktasında ilgili departmanların spesifik bilgi varlıklarının hangi özgün IT desteğine ihtiyaç duyacağının belirlenmesi ve bilgi güvenliği kontrollerinin yapılmasına yardımcı olmaktadır. Her ne kadar bilgi varlıkları envanteri IT Sorumlusu tarafından idare edilmekte ise de kağıt ortamında tutulan kayıt ve varlıkların güvenliği de göz önünde tutularak gerekli tedbirler alınmalıdır.

2.6. Bilgi varlıkları mantıksal bağlantılar ve toplama yöntemleri kullanılmak suretiyle tanımlanmalıdır. Örneğin, bir İSG çalışması için toplanan bilgiler, bir dizi dizüstü bilgisayar, bir grup sürücü ve USB bellekler dâhil olmak üzere çeşitli ortamlarda tutulabilir. Bu durumda, her ortamı ve bunların nasıl güvenli tutulduğunu açıklayan bir girdi olarak kaydedilmelidir.

2.7. Her ilgili departman bünyesinde tuttuğu bilgi varlıklarını beyan ederek envantere kaydedilmelerini sağlamalıdır. Dijital/kayıt depolama amacıyla yerel olarak alınan her bir ek depolama sistemi “Departmanca kullanılan sistem” varlığı olarak kaydedilmelidir. Ek bilgi varlıklarının kaydedilip kaydedilmesi gerektiği hususunda şüpheye düşülmesi halinde IT Destek Ekibi ile irtibata geçilmelidir. Bulut depolama sistemleri ve kâğıt ortamında tutulan dosyalama sistemleri de bilgi varlığı olarak tanımlanarak envantere kaydedilmelidir.

2.8. Departmanlarının bilgi varlıklarını gözden geçirirken Departman Şefleri aşağıdaki hususları göz önünde bulundurmalıdır:

- Envantere eklenmesi gereken herhangi bir bilgi varlığı mevcut mudur?

- Kullanılmayan ve envanterden çıkarılması gereken her hangi bir bilgi varlığı söz konusu mudur?
- Bilgi varlıkları envanterindeki kayıtların güncellenmesini gerektirecek bilgi varlıklarının kullanımı ile ilgili bir değişiklik söz konusu mudur?

- Departman tarafından kullanılan bilgi varlıklarının toplanma, işlenme biçiminde değişiklik ön gören her hangi bir politika değişikliği ya da yasal düzenleme söz konusu mudur?

2.9. Departman Şefleri, departmanlarındaki personelin birlikte çalıştığı tüm bilgiler veya bu bilgilerin saklandığı tüm unsurlar hakkında kapsamlı bilgiye sahip olmayacağı kabul edilmektedir. Departmanların, bilgi varlık kaydını tamamlarken departmanın elinde tuttuğu bilgilerle ilişkili temel riskler ve bu bilgilerin nerede saklandığı hakkında geniş bir şekilde düşünmeleri önerilir. Bölümler, özellikle verilerin hassas olduğu veya Kolej dışına aktarıldığı durumlarda veri aktarımına odaklanmayı faydalı bulabilir. Daha fazla rehberlik için lütfen IT Güvenlik Ekibi ile iletişime geçin.

3. BİLGİ VARLIKLARI ENVANTERİNİN YAPISI

Alan Adı	Açıklamalar
Bilgi Varlığı Sahibi	Bu bilgi varlığında depolanan bilgilerden kim sorumludur ve bu bilgi varlığıyla ilgili yapılacak sorgular için iletişim noktası/irtibat görevlisi kimdir?
Bilgi Varlığı Yöneticisi	Bilgi Varlığı Yöneticisinin üstleneceği rol BGYS Çerçeve Politika Metninde tanımlanmış olup bilgi varlığını günlük bazda kullanan en yetkili görevli olarak tanımlanabilir.
Bilgi Varlığının İsmi	Bilgi Varlığına atanan özgül isim
Bilgi Varlığının Tarifi	Bilgi varlığına ilişkin kısa bir tanımlama yapınız. Mümkün ise varlık bünyesinde tutulacak olan bilgilere ilişkin kısa bir bilgilendirme notu yazınız.
Varlığın Güncel Durumu	Yalnızca Bilgi Varlıkları envanterinde-Geçici, Onaylanmış ya da aktif değil vb.
Sınıflandırma	• Bilgi varlığı özel nitelikli veri ihtiva etmekte midir? Bu verilerle alakalı riskler nelerdir? Risklerin elimine edilmesi veya azaltılması için alınan tedbirler nelerdir? Özel nitelikli veriler olarak değerlendirilecek olan veriler aşağıdaki gibidir: o Ticari açıdan hassas veri olarak değerlendirilen Şirket idaresine ilişkin veriler ya da araştırma

	verileri. o 6698 sayılı Kanunun 6. Maddesinde belirtilen "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 mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri". o Bireysel finans verileri o Şirketin yaptırdığı Araştırma Geliştirme çalışmalarına ilişkin veriler. o Yukarıda yer almamakla birlikte ifşa edildiği takdirde ilgili kişilerin zarar görmesine ya da itibarının zedelenmesine neden olabilecek kişisel veriler de bu kategoride değerlendirilmelidir.
Varlığın Depolanacağı Ortam Türü	Elektronik, manuel ya da her ikisi
Kanuni Dayanak	İlgili verinin işlenmesi ve/veya depolanması için kullanılan yasal dayanak nedir? 6698 Sayılı Kanun gereği kişisel verilerin hukuka uygun olarak işlenebilmesi için veri sorumluları tarafından kullanılabilen meşru veri işleme sebepleri göz önüne alınmalıdır.
İş Akışı Açısından Taşıdığı Önem	Bilgi varlığının şirketin iş akışı açısından taşıdığı hayati önem düzeyi ve varlığın kaybı ya da gizliliklerinin ihlal edilmesi durumunda ortaya çıkacak olumsuzluk seviyesi
Bilgi Varlığının Konumu	Bilgi varlığı fiziksel olarak nerede muhafaza edilmektedir? Örneğin yerel bilgisayarlarda, merkezi sistemde, portal nezdinde ya da sunucu haricinde bulunan bir noktada
Bilgi Varlığını Ekleyen Taraf	İlgili kaydın Bilgi Varlıkları Envanterine girişini yapan kimdir?
Ön Görülen Depolama Süresi	Bilgi varlığı hangi süreyle envanterde tutulacaktır? Bilginin Şirket operasyonları açısından gerekli olmadığını tespit etmek ve güvenli bir şekilde imha edilmesi için ön görülen süreç nedir? Verilerin hangi süreden sonra imha edilmesi gerektiği hususunda Şirketin Veri Saklama ve İmha Politikasını inceleyiniz.
En Eski Girdi	Güncel tarih-saklama süresi aralığı içinde olmaması gereken en eski kaydın tarihi
En Son Kayıt Girdisi	Artık güncellenmesi yapılmayan bilgi varlıkları için son kaydın yapıldığı tarihi

Bilgi Varlığı Sahibi olarak atanan görevlilerin ayrıca aşağıda sıralanan hususları göz önünde bulundurması gerekmektedir:

- Sorumlu Birim: hangi birim bahse konu bilgi varlığından sorumludur? (Genellikle "varlık sahibinin" görevli olduğu birim)
- Bilgi varlığına erişim sağlayacak olan birim ve/veya görevliler? İlgili bilgi varlığına erişim sağlaması ön görülen kişi gruplarını belirtiniz. Örneğin belirli bir ekipte görevli çalışanlar ya da tüm şirket çalışanları. Ayrıca Şirket çalışanı olmamakla birlikte ilgili bilgi varlığına erişim sağlaması ön görülen üçüncü taraflar da açık bir şekilde belirtilmelidir.
- Bilgi varlığının güvenliği nasıl sağlanacaktır? Bilgi varlığının güvenliğini sağlamak için alınan tedbirleri özetleyiniz. Örneğin şifre ile koruma. Özel nitelikli kişisel veri ihtiva eden kâğıt ortamında tutulan kayıtlar kilitli bir dosyalama sisteminde muhafaza edilmekte midir? Kilitler ne şekilde muhafaza edilmektedir? Uyarı: kesinlikle kullanılan şifre ya da kilitlerin tutulduğu konumu belirtmeyiniz!
- Yedekleme, Mukavemet ve Afet Kurtarma düzenlemeleri: Verilerin kaybı ya da veri/sistem(ler) güvenliğinin ihlali ile afet, deprem vb. hallerde verilerin kurtarılması ve/veya işlevsellik ve erişilebilirliklerinin korunması için alınan tedbirler nelerdir?