BAYKARA KELEPÇE SAN. VE TİC. LTD. ŞTİ.

VERİ GÜVENLİĞİ PROSEDÜRÜ

Versiyon: 0

VERİ GÜVENLİĞİ PROSEDÜRÜ

1. Amaç ve Kapsam

Kanun'un 12. Maddesi ile veri sorumlusunun;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu düzenlenmiştir.

İşbu Doküman ile Kanun ile belirlenen ilkeler doğrultusunda Şirket tarafından oluşturulacak veya oluşturulmuş olan bilgi güvenliği ile ilgili politika ve prosedürlerde kişisel verilerin korunması ile ilgili gerekli düzenlemelere yer verilmesinin sağlanması ve kişisel verilerin korunması politika ve prosedürleri ile bağlantılı bir şekilde güvenlik ile ilgili önlemlerin oluşturulması amaçlanmaktadır.

İşbu Doküman, kıdemine ve teşkilat yapısındaki hiyerarşik konumuna bakılmaksızın tüm Çalışanların, Şirketimiz faaliyetleri esnasında Kişisel Veri güvenliği konusunda dikkate alması gereken hususları belirlemek için hazırlanmıştır. İşbu Dokümanda düzenlenen ilkeler ve Kişisel Veri Güvenliği ilkeleri tür, format kapsam ve benzeri bir ayrım yapılmaksızın Kişisel Verileri içeren bütün süreçlere uygulanır.

2. Kişisel Veri Güvenliği Esasları

Kişisel Verilerin hukuka uygun işlenmesi ve Kişisel Veri Güvenliği konusunda uluslararası kabul gören standartlar olan ISO 29100 ve BS 10012'e, Kişisel Veri Güvenliği ilkelerine ve Kanun ile belirlenen teknik ve idari tedbirlerin yerine getirilmesi yükümlülüğüne uyum sağlanması bakımından aşağıdaki ilkelere uyumlu çalışmalar gerçekleştirilmektedir:

- Kişisel Veri, yetkisiz erişim, imha, değişiklik, ifşa veya kayıp gibi risklere karşı Şirket'in hâkimiyeti altında ve Kişisel Verinin Bütünlüğü, Gizliliği ve Kullanılabilirliği korunmasını teminen alınacak operasyonel, işlevsel ve stratejik seviyelerdeki Kontrollerle korunabilir.

- Şirket, gerçekleştireceği işlemler kapsamında, Kişisel Veri Güvenliğinin sağlanması ve Kanunla uyumluluk açısından gerekli idari ve teknik tedbirleri yeterli seviyede alan Veri İşleyenlerle çalışmak konusunda gerekli özeni göstermektedir.

- Şirket, söz konusu Kontrolleri etkin biçimde uygulayabilmek adına bu Kontrolleri yürürlükteki mevzuata, uluslararası kabul gören güvenlik standartlarına, düzenli risk değerlendirmeleri neticesinde oluşturulan sonuçlara ve kar/maliyet dengesine göre tesis edebilir.

- Şirket, söz konusu Kontrolleri, Gizlilik ihlali riski ile doğru orantılı olarak, Kişisel Verinin hassasiyet seviyesi, etkilenebilecek Veri Sahibi sayısı ve Kişisel Verilerin işlendiği bağlamı dikkate alarak tesis etmektedir.

- Şirket, Kişisel Verilere erişimi sadece görevleri icabı bu verileri işlemesi gereken Çalışanlarla sınırlı tutmakta, bu Çalışanların da sadece kendi görevlerini ifa etmeleri için gerekli olan kişisel verilere erişmesi sağlanmaktadır.

- Yapılacak risk değerlendirmeleri neticesinde belirlenen riskler ve zayıflıklara ilişkin çözümler üretilmek suretiyle tedbirler alınmaktadır.

- Belirlenen Kontroller periyodik incelemelere, yeniden değerlendirmelere ve devamlı risk yönetimi süreçlerine tabi tutulmaktadır.

Yukarıda belirtilen ilkelere uyumun sağlanması amacıyla; Şirket faaliyetleri kapsamında gerçekleştirilecek olan Kişisel Veri işleme faaliyetlerine ilişkin olarak Kanun, en iyi sektör uygulamaları ve bilgi güvenliği konusunda genel kabul görmüş uluslararası standartlar göz önüne alınarak Kişisel Veri Uyumluluk Programı oluşturulmuştur. Bu Uyumluluk Programı yukarıda bahsedilen Kanun ve sair ikincil mevzuat, uygulamalar ve standartlarda meydana gelecek değişikliklerin yanı sıra Kurul kararları ile Kurul tarafından "Yeterli Korumanın Bulunduğu Ülke" olarak tespit ve ilan edilen ülkelerin Kişisel Verilerin Korunması konusunda yetkilendirilmiş makamlarının karar ve uygulamaları çerçevesinde gerek görüldükçe ve en geç Yönetim ve Denetim Prosedürü uyarınca yapılacak denetimler sonucunda güncellenecektir.

Buna ek olarak Şirket, Uyumluluk Programı kapsamında oluşacak pozisyonlara Kişisel Verilerin güvenliğini temin etme amaçlı olarak yetkin kişileri getirecektir. Şirket tarafından gerek Kanun gerekse Şirket tarafından Uyumluluk Programı çerçevesinde kabul edilip uygulamaya konulan politika ve prosedürler dahil diğer dokümanlarda belirlenen usul ve esaslara uygun şekilde Kişisel Veri Güvenliğinin sağlanması için uyulması hedeflenen Kişisel Veri Güvenliği unsurları aşağıda açıklanmaktadır.

a. Kişisel Verilerin Hukuka Aykırı İşleme ve Erişimin Engellemesi

Şirket'in Kişisel Verilere hukuka aykırı erişimi engellemek için alınan başlıca idari ve teknik tedbirleri belirlemesi gerekir. İşbu başlık altında, Kanun uyarınca Kişisel Verilere hukuka aykırı erişim sağlanmasının önlemesi amacıyla alınan tedbirler sıralanmaktadır.

i. Çalışanlar

- Çalışanlar, işleriyle ilgili olarak gerçekleşen faaliyetler kapsamda, Kişisel Verileri, Kanun hükümlerine ve Kişisel Veri İşleme Politikalarına1 aykırı olarak üçüncü taraflara açıklayamayacakları ve işleme amacı dışında söz konusu Kişisel Verileri kullanamayacakları ve bu yükümlülüğün görevden ayrılmalarından sonra da devam edeceği konusunda bilgilendirilmektedir. Çalışanların iştigal konularının Gizlilik ihlali riski yaratma ihtimali ile doğru orantılı olarak, uygun görülmesi halinde Çalışanların Taahhüt Metni imzalaması istenebilecektir.

    - [Referans: Taahhüt Metni]
    - [Referans: Yönetim ve Denetim Prosedürü - Eğitim]

ii. Veri İşleyenler

- Şirket, Veri Koruması Güvenliği ve Kanunla uyumluluk açısından gerekli idari ve teknik tedbirleri yeterli seviyede alan Veri İşleyenlerle çalışmak konusunda gerekli özeni gösterir.

- Şirket, Veri İşleyen ile veri paylaşılmasını gerektiren bir hukuki ilişki içine girmesi durumunda; Veri İşleyen tarafından alınması ve uygulanması gereken asgari tedbirlerin neler olduğuna ve bu tedbirlere uyulmasına ilişkin hükümleri içeren bir sözleşme yapar. Mevcut sözleşmelerin, Kişisel Veri Güvenliği bakımından arz ettiği risk seviyesine göre, (i) sözleşmelere konuyla ilişkili protokol eklenmesini (ii) veya sözleşmelerin yenileme dönelerimde uygun şekilde tadil edilmesini temin eder.

- Şirket Veri İşleyenden, Veri İşleyenin kendi çalışanlarına (iştigal konularının Gizlilik ihlali riski yaratma ihtimali ile doğru orantılı olarak belirlenecek çalışanlara) gizlilik ve güvenlik hususlarını içeren bir taahhüt metni imzalatasını şart koşabilir.

- Şirket, Kişisel Veri Güvenliği açısından oluşabilecek problemlerin ağırlığı ve olasılığı ile orantılı olarak belirleyeceği şartla göre, Veri İşleyenlerin faaliyetleri üzerinde denetim hakkı talep eder. Denetim hakkı, oluşabilecek problemlerin ağırlığı ve olasılığı ile orantılı olarak saha denetimi ya da uluslararası kabul gören standartlara uyumluluk beyanı şeklinde olabilir.

- Şirket, yalnızca faaliyetlerini yerine getirmek amacıyla gereksinim duyduğu asgari seviyede Kişisel Verinin Kanun'a uygun işlenmesini temin etmek üzere, Veri İşleyene verilerin işlenme amacını açıkça sınırlarını çizmek suretiyle bildirir.

    - [Referans: Çerçeve Sözleşmeler]

[1] Şirket Çalışanları için Kişisel Verilerin Korunması ve İşlenmesi Politikası ile Şirket Kişisel Verilerin Korunması ve İşlenmesi Politikası

- [Referans: Kişisel Veri Aktarımını ve İşlenmesini İçeren Sözleşmeleri İnceleme Klavuzu – CheckList]

iii. Kontroller

Şirket, Kişisel Verilerin işlenmesi ve muhafaza edilmesi için tesis edeceği güvenlik önlemlerini ve Kontrolleri belirlerken uluslararası uygulamalarda kabul edilmiş ilkeler ışığında hareket etmektedir. Buna istinaden işlenecek Kişisel Verinin özellikleri ile hassasiyet derecesine göre farklı Kontroller tesis edilebilecektir. Bu süreçte Şirket tarafından sağlanacak ürün ve hizmetlerin oluşturulması aşamasında, baştan tesis edilmiş ilke ve Kontrollerin dikkate alınarak sürecin ilerletilmesinin Kişisel Veri Güvenliği İhlal Olayı oluşma ihtimalini azaltabileceği düşünülmektedir.

Kontrollerin oluşturulması ve uygulanması sırasında burada belirlenen uluslararası kabul görmüş ilkelerin, somut olayların özellikleri de dikkate alınarak mümkün mertebe göz önünde tutulmasının, sürekli olarak takip edilmesinin ve yeri geldiğinde genel kabul görmüş uygulamalara uygun olarak güncellenmesinin iyi bir risk yönetim mekanizması kurulması için önem arz ettiği değerlendirilmektedir

- Şirket, hukuka aykırı erişimin ve işlemenin engellenmesi için gerekli önleyici faaliyetleri belirler. Önleyici faaliyet olası uygunsuzlukların önlenmesi için yapılan bir faaliyet olması nedeniyle, Şirket faaliyetlerinin her aşamada gözden geçirilmesi sonucunda tespit edilebilecek bir durumdur. Bu nedenle herhangi bir çalışan, önleyici faaliyet isteğini herhangi bir zamanda yapabilir. Süreçlerin izlenmesi ve ölçülmesi çalışmaları veya denetim sırasında Komite kendisi ya da yapacağı görevlendirme ile üçüncü bir kişi tarafından güvenlik açığı eğilimlerini gözden geçirerek, olası uygunsuzlukların çıkabileceği durumları tespit ettiğinde ilgili birim sorumlularından önleyici faaliyet isteğinde bulunabilir.

- Şirket tarafından, hukuka aykırı erişimin ve işlemenin engellenmesi için gerekli önleyici faaliyetleri belirlenmesini takiben belirlenen bu noktalara ilişkin Kontroller oluşturulur ve Kontrollerin belirlenen periyodik dönemlerde gerçekleşmesi ve buna ilişkin Kontrol raporlarının yazılmasına ilişkin gerekli tedbirleri alır. Kontrol raporları, asgari olarak her denetim sonrasında gerçekleştirilir.

- Şirket, Kişisel Verilere erişim ile ilgili denetim izlerini tutarak yetkisiz erişimlere karşı sürekli gözetleme yapar.

b. Kişisel Verilerin Muhafazası

Şirket Kişisel Verilerin muhafazası yükümlülüğünü en iyi sektör uygulamaları ve bilgi güvenliği konusunda genel kabul görmüş uluslararası standartlar göz önüne alınarak yerine getirmektedir.

- [Referans: Kişisel Verilerin Saklanması Politikası]

c. Veri Güvenliği İhlali

Şirket tarafından işlenen Kişisel Verilerin hukuka aykırı olarak işlendiğinin veya bu verilere yetkisiz bir şekilde erişildiğinin veya veri güvenliğinin tehdit altında olduğunun tespit edilmesi halinde; ihlalin ortadan kaldırılması için gerekli önlemler derhal alınır. Kişisel Verinin hukuka aykırı bir şekilde 3. Kişi tarafından elde edilmesine dayalı İhlal Olayı'nda söz konusu olay hakkında ilgililere bilgi verilir.

- [Referans: Yönetim ve Denetim Prosedürü – Kişisel Veri Güvenliği İhlal Olayı Yönetimi]

d. Denetim

Uyumluluk Programı dahilinde Kişisel Verilerin hukuka uygun bir şekilde işlenmesinin sürdürülmesi ve risklerin tespit edilerek gerekli kontrollerin uygulanmasının sağlanması amacıyla Şirket atarfından sürekli denetimler gerçekleştirilmektedir.

- [Referans: Yönetim ve Denetim Prosedürü - Denetim]

e. Eğitim

Şirket içerisinde Kişisel Verilerin korunması konusunda yasal yükümlülüklerin öğrenilmesi ve farkındalığın arttırılması adına Şirket Çalışanlarına eğitim verilmektedir.

- [Referans: Yönetim ve Denetim Prosedürü - Eğitim]

3. Kişisel Veri Güvenlik Önlemleri

Kişisel Veri Güvenliği Esaslarının uygulanması adına alınacak Kişisel Veri Güvenlik Önlemleri, Kişisel Verilerin işlendiği ve muhafaza edildiği ortamın fiziksel özelliklerinden bu Kişisel Verilerin transferinde alınacak önlemlere kadar geniş bir yelpazeyi kapsamaktadır.

a. Kişisel Veri İşleme, Muhafaza Etme, Paylaşmada Kullanılan Araçlara İlişkin Esaslar

Kişisel Verilerin işlenmesi ve muhafaza edilmesi için kullanılan araçlara ilişkin olarak Çalışanlar, kendilerine verilen eğitimler çerçevesinde gerekli teknik ve operasyonel önlemleri alacaklardır. Bu araçların yetkisiz erişimlerden korunması için çeşitli önlemler alınabilecektir.

Kişisel Verilerin işlendiği, muhafaza edildiği, Kanun'a uygun olarak üçüncü kişilere aktarıldığı araçlarda ve aktarım süreçlerinde genel kabul gören en iyi sektör uygulamaları ile uluslararası standartlarda belirlenen Kontroller uygulanır. Özellikle uygun düştüğü ölçüde Kişisel Veri muhafaza edilirken veya aktarılırken işbu Prosedür'de bulunan Şifreleme esasları uygulanabilecektir. Buna ek olarak aşağıdaki kurallara uyulmasının Kişisel Veri Güvenliği İhlal Olayı ihtimalini azaltacağı düşünülmektedir:

Kağıt ortamındaki kişisel veriler:

- Kişisel Veri içeren dokümanların fiziksel kopyalarının kilit altında, yetkisiz erişimleri engelleyecek şekilde tutulması, mümkün mertebe dijital ortama aktarılması, fiziksel olarak kullanılma gereksinimi sona erenlerin güvenli ortamda imha edilmesi,
- Fotokopi makinalarının Kişisel Veri içeren bir doküman basımında kullanılması halinde makinanın boş bırakılmaması, yetkisiz kişilerce bu Kişisel Verilere fiziksek erişim sağlanabilecek durumlardan kaçınılması, basılan veya kopyalanan dokümana ait tüm kopyaların makinadan alındığından emin olunması,
- Fotokopi makinalarında basılan veya kopyalanan Kişisel Veri içeren dokümanların hatalı kopya / basım hallerinde hatalı kopyaların derhal imha edilmesi, makinada bırakılmaması,

Çalışan araçlarında işlenen kişisel veriler:

- Kişisel bilgisayar, e-posta, telefon vb. uygun cihazlara kullanıcı şifreleri koyulması,
- Kişisel bilgisayarların başında olunmayan her anda, bulunmama süresinden bağımsız olarak kişisel bilgisayarın kitlenmesi,
- Kişisel bilgisayarların masaüstü bölümlerinde mümkün olan en az sayıda dosyanın bulunması, bu dosyaların gerekli olduğu ölçüde şifrelenmesi,
- Çalışan'ın bizzat kullandığı araçlardaki Kişisel Verilerin, Şirket Uyumluluk Programı çerçevesinde oluşturulacak Veri Envanteri'ne göre sınıflandırılması, özellikle "Kamuya Açık", "Şirket içi", "Gizli", "Özel Nitelikli" şeklinde dosyalanması, gerekenlerin şifrelenerek saklanması,
- E-postalarda Kişisel Veri gönderilmesinden imtina edilmesi, gerekli olması halinde e-postanın şifrelenmesi, e-posta başlıklarında içerikte Kişisel Veri olduğu intibası uyandırabilecek ifadelerden kaçınılması,
- Alınan e-posta ve mesajların virüs taramasından geçirilmeden açılmaması,
- Özellikle taşınabilir dizüstü bilgisayarların toplantı, seyahat vb. nedenlerle Şirket dışına çıkarıldığı hallerde ilgili Çalışan'ın gözetiminden ayrılmaması, otel odası vb. yerlerde kilit altına alınmaksızın bırakılmaması.
- Kişisel bilgisayar, cep telefonu, e-posta ve benzeri araçların kullanıcı şifrelerinin üçüncü kişilerle paylaşılmaması, belirli aralıklarla yenilenmesi, doğum tarihi ve benzeri kolay bulunabilecek şekilde belirlenmemesi, herhangi bir yere yazılmaması
- Şirket'in gösterdiği ve izin verdiği haricinde Kişisel Veri içeren dokümanların herhangi bir bulut sisteminde barındırılmaması

Veri depolama araçlarında işlenen kişisel veriler:

- USB, harici bellek ve benzeri veri depolama araçlarının şifrelenerek kullanılması, ortalık yerde bırakılmaması, yetkisiz kişilerin erişimine karşı güvenli muhafaza edilmesi,

- USB, harici bellek ve benzeri veri depolama araçları içerisinde Kişisel Veri içeren, dijital olarak "bozulmuş" veya "deforme olmuş" dosyaların güvenli ve geri dönülemez şekilde imha edilmesi,
- USB, harici bellek ve benzeri veri depolama araçlarının çalınması, kaybolması ve benzeri hallerde derhal ilgili iş birimi sorumlularının bilgilendirilmesi,
- USB, harici bellek ve benzeri veri depolama araçlarının, e-postaların, kişisel bilgisayarda bulunan dosyaların şifreleme esaslarının ve anahtarlarının yetkisiz taraflarla paylaşılmaması,

b. Şifreleme

Kanun'un 12. maddesi kapsamında alınabilecek teknik önlemlerden birisi de bir verinin anahtar diye nitelenen matematiksel bir algoritma ile yalnızca bu anahtara erişim izni olan taraflarca görüntülenebilmesinin temin edildiği *şifreleme* yöntemidir. Şifreleme yönteminin bir verinin yetkisiz edinilmesini değil, yalnızca içeriğinin yetkisiz taraflarca görüntülenebilmesini engellediği göz önüne alınarak bu yöntemin, alınan diğer teknik ve idari önlemlerin tali ve tamamlayıcı bir unsuru olarak Kişisel Veri Güvenliği'ni tesis etmek üzere kullanılabileceği dikkate alınmalıdır. Özellikle son yıllarda uzaktan iletişim araçlarının teknolojik gelişmeler ışığında çeşitlenmesi ile veriler, taşınabilir depolama cihazları içerisinde muhafaza edilebilmektedir. Bu husus, ilgili cihazlarda depolanan verilerin Kanun ve diğer uygulanabilir düzenlemeler ışığında mevzuata uygun ve etkin bir biçimde korunması gerekliliğini ortaya koymaktadır.

i. Şifreleme Yöntemleri

Şirket'in şifreleme yöntemini kullanmayı tercih etmesi halinde, işbu Prosedür'de açıklanan şekillerde açık (asimetrik) veya gizli (simetrik) şifreleme yöntemlerinden birini kullanması tavsiye olunur. Bu tercihinde iş ve veri akışlarının gereklerine göre değişiklik yapabilecektir. Herhangi bir uygulanabilir mevzuat kapsamında güvenliğinin şifreleme yöntemi ile tesis edilmesi gerekliliği doğrudan ya da dolaylı olarak belirtilen veriler her halükarda şifrelenecektir.

Açık (Asimetrik) Şifreleme:

Herkesin erişimine müsait olan açık anahtar ile verinin şifrelenmesi, ilgili açık anahtarın matematiksel algoritma olarak eşleştiği ve yalnızca bir veya sınırlı kişinin sahip olduğu gizli anahtar ile ilgili verinin deşifre edilmesi işlemidir. Gizli anahtar olarak dijital imza da kullanılabilecektir. Veriye erişim ve işleme yetkisi olacak tarafların güvenli ortamda ilk anahtar değişimi yapmasının mümkün olmaması veya zor olması hallerinde açık şifreleme kullanılması, daha güvenli olması açısından tercih edilebilir.

Gizli (Simetrik) Şifreleme:

Yalnızca belirli kişilerin uhdesinde olan birebir aynı tek bir anahtar veya basitçe birbirine dönüştürülebilecek iki anahtar ile verinin hem şifrelenebilmesi hem de deşifre edilebilmesi işlemidir. Veriye erişim ve işleme yetkisi olacak tarafların güvenli ortamda ilk anahtar değişimi yapmasının mümkün olduğu ve Şirket tarafından uygun görüldüğü ölçüde yüksek seviyede güvenlik sağlar. Bu yöntem, dizi şifreleri veya blok şifreleme tiplerinden biri seçilerek yapılabilir.

ii. Şifreleme Esasları

Şifreleme yönteminin kullanılması ile hem taşınabilir hem de diğer cihazlar içerisinde depolanan bilgilerin yetkisiz erişim ve işlemelere karşı korunması amaçlanmaktadır. Şirket, her bir iş ve veri akışı bazında uygun şifreleme yöntemlerini ayrı ayrı belirleyip uygulayabilir. Bu halde Kişisel Veri Güvenliği İhlal Olayı oluşma ihtimalinin ve muhtemel etkilerin asgari düzeye indirilmesi adına şifrelemeye dair anahtarın yalnızca yetkili çalışanlar ile paylaşılması uygun görülmektedir. İş ve veri akışlarına göre belirlenen her bir şifreleme yönteminde şifreleme anahtarları sürelik periyotlarda yenilenir. Şifreleme yöntemi ve bunun altında hangi şifreleme metodu kullanılırsa kullanılsın şifreleme işlemi bu konudaki uluslararası sektör ve bilgi güvenliği standartlarına uygun biçimde yapılmalıdır.

Veri Depolamaya Dair Şifreleme Uygulama Esasları:

Dizüstü bilgisayar, masaüstü bilgisayar sabit diski, USB cihazları, harici bellekler, dosya sunucuları, yedekleme sistemleri Şirket tarafından uygun görülen ölçüde tamamının şifrelenmesi (full disk encryption) veyahut ilgili dosyaların ayrı ayrı şifrelenmesi (individual file encyription) yöntemleri ile şifrelenebilir. Özellikle bu cihazların büyük ölçüde kişisel veri barındırması halinde ilgili cihazın tamamının şifrelenmesi etkili olabilecektir.

Buna ek olarak kişisel veri barındıran veri tabanlarının da tamamının şifrelenmesi tavsiye edilir. Bir cihazın tamamının şifrelenmesinin mümkün olmadığı hallerde asgari olarak kişisel veri içeren dosya ve materyallerin şifrelenmesi, şifreleme sonucunda ilgili anahtarların yalnızca yetkili çalışanların uhdesinde kalması yolu tercih edilebilir. Kanun ve diğer uygulanabilir düzenlemelere göre işlenebilen verinin, işleme süresince şifrelenmiş şekilde muhafaza edilebilmesi halinde bu şekilde işlenmesi; aksi takdirde şifre, veri işleme esansında şifreleme anahtarı ile okunabilir hale getirilip işlemenin bitmesini takiben tekrar aynı anahtar ile şifrelenmesi etkin bir koruma sağlayacaktır. İlgili çalışanların deşifre edilmiş veri üzerinde çalışırken ilgili cihazları tekrar şifreleme yapmaksızın terk etmemesi konusunda çalışanlar bilgilendirilecektir.

Veri Transferine Dair Şifreleme Uygulama Esasları:

Kişisel verilerin herhangi bir şekilde internet bağlantısı veya benzeri şekillerde bir taraftan başka bir tarafa gönderilmesi halinde hem ilgili verinin ve/veya dosyanın şifrelenebilecek olmasının yanı sıra aynı zamanda da şifrelenmiş bir güvenli internet iletişim protokolü kullanılarak transfer edilmesi tavsiye olunmaktadır. Gönderilen e-posta başlıklarında kişisel veri, özellikle hassas kişisel veri olmamasının temin edilmesi yönünde gayret gösterilmesi, e-posta metni veya eki kişisel veri içeriyor ise metin veya dosya ekinin şifrelenmesi ve de şifrelenmiş, güvenli bir internet iletişim protokolü kullanılarak transfer edilmesi ihlal risklerini asgari düzeye çekeceğinden tavsiye edilir.

c. Veri Paylaşımı

Herhangi bir üçüncü kişi ile veri paylaşımı gerçekleştirmeden önce aşağıdaki soruların cevaplanması önem arz edecektir:

- Paylaşımın amacı nedir?
- Paylaşılması söz konusu olan veriler nelerdir?
- Veriye erişim sağlayacak taraf(lar) kim(ler)dir? Bu taraf(lar), yurtiçinde mi yurtdışında mı bulunmaktadır?
- Paylaşım ne zaman(lar)da ve sıklıkta yapılacaktır?
- Paylaşım yöntemi nedir?
- Paylaşım neticesinin amacına uygun olup olmadığının denetlenmesi mümkün müdür? Bu denetim ne şekilde yapılabilir?
- Veri paylaşımı herhangi bir risk ortaya çıkarmakta mıdır? Çıkardığı risk nedir?
- Veri paylaşımı söz konusu olmaksızın veya veri anonim hale getirildikten sonra paylaşılarak da aynı amaca ulaşılması mümkün müdür?
- Paylaşım, ilgili veri sahibinden alınmış olan rızaya veya veri sahibine yapılmış olan bilgilendirmeye uygun mudur?

Bahsi geçen soruların cevaplanması sonrasında veri paylaşımına karar verilmesi halinde,

- Kişisel veri paylaşımının yasal dayanağı (Kanun kapsamında açık rıza gerektirip gerektirmediği) tespit edilmeli,
- Daha önce alınan onay / yapılan bilgilendirme kapsamı dışında bir paylaşım söz konusu ise ilgili veri sahibinden kişisel veri paylaşımına uygun bir onay alınmalı veya veri sahibine gerekli bilgilendirme yapılmalı,
- Kişisel verinin aktarılacağı üçüncü kişi ile veri paylaşımına ilişkin olarak bir sözleşme* akdedilmelidir.

4. Tanımlar

Bütünlük	:	Kişisel Veri'nin doğruluğunu ve tamlığını koruma özelliği
Çalışanlar	:	Şirket Çalışanları
Gizlilik	:	Kişisel Veri'nin yetkisiz kişilere ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği
Kanun	:	6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kişisel Veri	:	Kanun kapsamında bulunduğu sürece, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Veri Güvenliği	:	Kişisel Veri'nin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması (ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar)

Kişisel Veri Güvenliği İhlal Olayı veya İhlal Olayı	:	Şirket'in Kanun'la uyumluluğunu ve Kişisel Veri Güvenliğini tehlikeye atma veya tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı
Kontrol	:	Kişisel Verilerin işlenmesi esnasında ortaya çıkabilecek Kişisel Veri Güvenlik İhlal Olaylarına bağlı risklere ilişkin olarak uygulanan en iyi sektör uygulamaları, Şirket politikaları ve prosedürleri, Uyum Programları, teknik ve teknolojik rehberler ve organizasyon yapısı gibi idari, yönetsel, teknik veya hukuki koruma ve karşı önlem yöntemleri
Komite	:	Kişisel Verilerin Korunması Komitesi
Kullanılabilirlik	:	Kişisel Veri'nin Çalışan ya da Veri Sahibi tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği
Kurul	:	Kişisel Verileri Koruma Kurulu
Kurum	:	Kişisel Verileri Koruma Kurumu
Prosedür	:	İşbu Yönetim ve Denetim Prosedürü
Üst Kurul	:	Kişisel Verilerin Korunması Üst Kurulu
Uyum Programı	:	Şirket tarafından yürürlüğe konulmuş, Kanun ile uyumluluğun sağlanmasına ilişkin program
Veri Envanteri	:	İş Birimi Faaliyetleri Bazlı Kişisel Veri İşleme Haritası ve Envanteri
Veri İşleyen	:	Tedarikçiler, danışman şirketler, taşeron şirketler dâhil fakat bunlarla sınırlı olmamak üzere Kanun'da tanımlı şekilde, Şirket'in verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Sahibi	:	Kişisel verisi işlenen gerçek kişi
Veri Sorumlusu	:	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi