KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

A. POLİTİKA, KAPSAM, AMAÇ

Kişisel Verileri Saklama ve İmha Politikası ("Politika"), DEARSAN GEMİ İNŞAAT SANAYİ A.Ş. ("**Şirket**") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Bu kapsamda Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler, diğer üçüncü kişilere ait kişisel veriler ve şirket verilerinin T.C. Anayasası, uluslararası sözleşmeler, 6689 Kişisel Verilerin Korunması Kanunu ("**Kanun**") ve diğer ilgili mevzuata uygun olarak işlenmesi, saklanması, silinmesi, yok edilmesi veya anonim hale getirilmesi işbu Politikaya uygun olarak gerçekleştirilir.

1. Kapsam

Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Şirketin sahip olduğu ya da Şirketçe yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

B. TANIMLAR

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,
İlgili Kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,
Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,
Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.
İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemini,
Periyodik İmha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,
Kişisel verinin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,
Kişisel Verilerin Anonim Hale Getirilmesi: kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemini,
Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,
Karartma: Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri,

De-manyetize etme: Manyetik medyanın özel bir cihaz kullanılarak manyetik alana maruz bırakılarak verilerin okunamaz şekilde bozulmasını,
Fiziksel Yok Etme: Ortamların, kırpıcı, öğütücü gibi cihazlar kullanılarak toz haline getirilmesini,
Üzerine Yazma: Üzerine yeniden yazılabilir ortamların üzerine özel yazılımlar kullanılarak en az 8 9 kez rastgele verilerin yazılarak eski verinin kurtarılamaz hale getirilmesini ifade eder.

C. POLİTİKA

1. Saklama Politikası

- Tüm veriler ilgili bilgi güvenliği ve kişisel veri sınıfına göre uygun koşullarda saklanmalıdır.
- Her tür sistemde, uygulamada ve fiziksel ortamlarda bulunan verinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması için erişim yetkilendirme yapılmalıdır. Tüm sistem, uygulama ve fiziksel ortamlara yönelik erişim yetkilendirme kural ve süreçleri Erişim Yönetimi Talimatı içerisinde detaylandırılmıştır.
- Saklama ortamlarının güvenliğinin sağlanması için uygun koşullarda fiziksel güvenlik önlemleri alınmalıdır.
- Elektronik dokümanlar, ilgili bölümlerin sorumluluğunda hemen ulaşılabilecek şekilde düzenli bir klasör yapısı içerisinde tutulmalıdır. Klasörlere, çalışanların bilmesi gerektiği kadar prensibi ile erişim yetkilendirme yapılmalıdır. Dosyalara erişim kontrol altında tutulmalıdır.
- Basılı dokümanları sınıflarına göre uygun güvenli muhafaza alanlarına konulmalıdır. Düşük güvenlik seviyeli dokümanlar açık dolaplarda, yüksek güvenlik seviyeli dokümanlar kilitli dolap veya çelik kasalarda olmalıdır.
- Elektronik ortamda bulunan tüm verilerin yedekleme işlemleri yapılmaktadır.

1.1. Saklama Ortamları

Kurumsal bilgiler ve kişisel verilerin bulunduğu ortamlar aşağıda bulunan ortamlar üzerinde kayıt altına alınmaktadır.

- Kağıt Ortam
- Dosya Sunucusu (File Server)
- Kurumsal Uygulama Veritabanları
- Ağ Cihazları

1.2. Saklama Sorumluluğu

Departman Müdürleri:
Kendi birimlerine ait basılı dokümanların fiziksel olarak gerekli güvenlik önlemleri alınarak saklanmasından sorumludur.

Arşiv Sorumlusu:
Arşive kaldırılması gereken doküman ve kayıtların düzenli olarak arşivlenmesi ve arşivdeki bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasından sorumludur.

Bilgi İşlem Müdürü:
Şirketin tüm kurumsal uygulama ve dosya sistemleri üzerindeki verilerin tüm altyapı ve sistemsel güvenliği sağlanarak ilgili saklama ortamlarında saklamak, periyodik olarak yedeklerini almaktan sorumludur.

1.3. Saklama Süreleri

Kişisel verilerin saklama süreleri, kullanım amacına göre değişiklik göstermektedir. Verilerin saklama sürelerine ilişkin detaylar "Kayıtların Yönetimi, Dosyalama ve Arşivleme Prosedürü" içerisinde ele alınmaktadır.

2. İmha Politikası

Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde imha edilir. Saklama ortamları yeterli özen gösterilmeden ve güvenlik tedbirleri alınmadan imha edildiğinde, şirket ve kişisel verilerin başka kişilerin eline geçme durumu söz konusu olabilir.

Dolayısıyla imha aşamasında ve daha sonrasında bu riski en aza indirmek için;

- Bilgi ve veri taşıyan cihaz ya da ortamların güvenli bir şekilde imhası için ilgili kanun ve yönetmelikler de göz önünde bulundurularak gerekli olması halinde süreç ve yöntemler belirlenmeli ve prosedürler hazırlanmalıdır.
- Şirket verileri ve kişisel veriler içeren saklama ortamları güvenli ve tehlike içermeyecek bir şekilde bu prosedürlere göre imha edilmelidir.
- İmha edilen tüm ortamların imha edildiğine dair kayıt tutulmalı ve 3 sene boyunca saklanmalıdır.
- İmha edilecek veriler Kişisel Veri sınıfına ve saklama ortamının tipine uygun olan yöntemler ile imha edilmelidir.
- İmha işlemi eğer Şirket dışında başka bir tedarikçi firma tarafından gerçekleştirilecekse, birçok kuruluş ortamlar için imha hizmetleri sunar fakat doğru yöntemler ile imha etmek teknik yeterlilik ve tecrübe gerektirir; dolayısıyla tedarikçi firma seçimine özen gösterilmelidir.
- Her türlü kişisel veri taşıyan cihaz ya da ortamların güvenli bir şekilde elden çıkarılabilmesi, imhası ve farklı uygulamalar için kullanımını sağlayacak hassas bilgi temizleme işlemleri için gerekli süreç ve yöntemler belirlenmeli ve belgelenmelidir. İşlemlerinin bu yöntemlere uyularak yapıldığı kontrol edilmelidir.
- Her türlü kişisel veri içeren basılı doküman imha edilirken kağıt kırpma makinası veya yakma yöntemi tercih edilmelidir.
- Sabit disklerin ve disketlerin formatlanması bilgilerin güvenli olarak temizlenmesi için yeterli değildir. Bu bakımdan formatlama yeterli bir güvenlik önlemi değildir.
- Her türlü kişisel veri içeren dokümanlar kullanım ömrü dolduğu zaman güvenli bir şekilde imha edilmelidir, geri dönüşüm amaçlı olarak biriktirilip değerlendirilmesi güvenlik açığı oluşmasına neden olabilir.

- Güvenli olarak tekrar kullanılır hale getirme ya da imha işlemleri tecrübeli personel ve tedarikçi firmalar tarafından yapılmalıdır.
- Yapılan tüm işlemler detaylı olarak kayıt altına alınmalıdır. Cihaz ya da depolama ortamını belirleyici bilgiler (tip, satıcı, model, seri numarası gibi), yapılan işlemin ne

amaçla yapıldığı ve kullanılacaksa işlem sonunda cihazın ya da depolama ortamının ne amaçla kullanılacağı, yapılan temizlik işleminin detaylı açıklaması (yapılan işlemler, kullanılan cihaz ve yazılımlar, vs.) ve işlemi yapan kişilerin bilgileri bu kayıtlarda yer almalıdır.

2.1. İmha Yöntemleri

Veriler, içerisinde bulundukları saklama ve kayıt ortamlarına ve gizlilik seviyelerine göre uygun yöntemler belirlenerek silinmelidir. İmha işlemi gerçekleştirilirken kullanılan yöntemler;

- Silme
- Yok Etme
- Anonimleştirme

olarak belirlenmiştir.

Silme: Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Yok Etme: Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

Anonimleştirme: Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Bu yöntemlerden herhangi biri kullanılırken uygulanacak belli başlı imha teknikleri bulunmaktadır. Güvenli bir imha gerçekleştirebilmek için verinin bilgi güvenliği ve kişisel veri sınıfına ve bulunduğu ortamın türüne uygun olan teknikler kullanılmalıdır.

Aşağıdaki tabloda, hangi ortam için hangi imha tekniğinin kullanılabileceği açıklanmıştır.

ORTAM	SİLME	YOK ETME	ANONİMLEŞTİRME
Dosya Sunucusu	Delete / Silme Komutu ile dosya silinir.	Sunucu içerisinde kullanılan diskler için; 1- De-manyetize etme (Degauss) 2- Fiziksel Yok Etme 3- Üzerine Yazma	**Uygulanmaz**
Veritabanları	Veritabanına göre uygun “DELETE” komutu ile kayıtlar silinir.	Veritabanı sunucusu içerisinde kullanılan diskler için; 1- De-manyetize etme (Degauss) 2- Fiziksel Yok Etme 3- Üzerine Yazma	Anonimleştirme yöntemlerinden; 1- Değişkenleri Çıkartma 2- Kayıtları Çıkartma 3- Alt ve Üst Sınır Kodlama 4- Bölgesel Gizleme 5- Örnekleme

Kağıt Ortam	Doküman üzerinde "Karartma" uygulanır.	Kağıt Öğütücü cihazlar kullanılır.	**Uygulanmaz**
Mobil Telefonlar (Sim Kart ve Hafıza Alanları)	Fabrika ayarlarına geri döndürme yapılır, tüm bellek ve hafıza kartları uygun yazılımlar kullanılarak silinir.	Telefon bellek ve hafıza kartları için; 1- Fiziksel Yok Etme 2- Üzerine Yazma	**Uygulanmaz**
Ağ Cihazları	"Delete / Sil " komutu kullanılabildiği durumlarda içerisindeki bilgiler silinir.	Silme yapılamadığı durumlarda; 1- De-manyetize Etme (Degauss) 2- Fiziksel Yok Etme 3- Üzerine Yazma tekniklerden biri uygulanır.	**Uygulanmaz**

2.2. İmha Sorumluluğu

Bilgi İşlem Departmanı:
Kişisel Verilerin, imha edilecek ortamlarda güvenli şekilde imha edilebilmesi için imha yöntemlerine ilişkin güvenli tekniklerin belirlenmesi aşamasında yönlendirme sağlamak.

İlgili Departman Müdürü:
Periyodik imha dönemlerinde, sorumluluğunda bulunan departmandaki imha edilmesi gereken şirket ve kişisel verilerin takibini yapmak ve imha sürecine dahil olmasını sağlamak.

KVK Komitesi/Temsilcisi :
İmha edilecek ortamların güvenli şekilde imha edilebilmesi için imha yöntem ve tekniklerin belirlenmesinden, uygulamaya geçilmesinden ve ortamların imha edilmesi için onay verilmesinden sorumludur.

2.3. İmha Metodolojisi

İmha sürecine ilişkin detaylar, "Kayıtların Yönetimi, Dosyalama ve Arşivleme Porsedürü" içerisinde detaylandırılmıştır.

Altı aylık periyotlar halinde imha gerçekleştirilir.

İlgili kişiler tarafından gelen imha talepleri, gerekli araştırmalar yapıldıktan sonra "Kayıtların Yönetimi, Dosyalama ve Arşivleme Porsedürü" ne göre imha edilir.

3. Politikanın Güncel Tutulması

Komite, kişisel verilerin saklanması ve imhası hakkında mevzuat ve sair ilgili mevzuat ve düzenlemelere ilişkin yenilik, değişiklik, gelişmeleri takip etmek ve bu doğrultuda Politika'yı güncel tutmakla yükümlüdür.

Doküman Sahipliği ve Onay

Bu dokümanın sahibi Komite'dir. Ayrıca Komite, işbu Politika'nın yukarıda belirtilen gözden geçirme gereklilikleri uyarınca düzenli olarak gözden geçirilmesinden sorumludur.

Bu dokümanın güncel versiyonu şirketin İnternet web sitesi üzerinde tüm çalışan personel ve ziyaretçilerin erişimine sunulmuş ve yayınlanmıştır.

İşbu Politika 15.09.2020 tarihinde Genel Müdür tarafından imzalanıp onaylanarak yürürlüğe girmiştir.