Kişisel Veri Yönetimi ve Güvenliği Politikası

AMAÇ

6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun olarak; Kişisel verilerin hukuka aykırı olarak elde edilmesi işlenmesini ve erişilmesini önlemek. Belirli, meşru ve açık amaçlar doğrultusunda işlenmiş olan kişisel veriler üzerindeki organizasyonel, teknik, idari, teknolojik, metodolojik kontrol ve önlemlerin alınmasını sağlamak.

KAPSAM

Merzifon Elektro Motor Metal Endüstri San. ve Tic. A.Ş. (Kurum) Kişisel Verilerin Korunması Kanunu'na uygun olarak alınmış ve işlenmiş veya işlenmekte olan kişisel verilerin ister dijital ortamda isterse fiziksel ortam kayıtlı olsun tüm farklı mekân ve ortamlardaki kişisel verilerin güvenliğinin sağlanmasıdır.

UGULAMA

1. Kurumda Kişisel Veri Güvenliği Yönetim Sistemi kurulmuştur. Her çalışan kişisel veri güvenliğine uygun çalışmaktan ve bilgi güvenliğine uygun davranmaktan sorumludur. Bilgi güvenliğine uygun çalışmayan ve belirlenmiş kurallara iş, işlem ve olaylar için "Bilgi Güvenliği Olay İhlal Formu" doldurarak kurumun veri güvenliğine katkıda bulunulur.
2. Kurum olarak Kişisel Verilerin Korunması Kanunu ve Kişisel Verileri Koruma Kurumu'nun yasal düzenlemelerine uygun olarak çalışmak için gerekli, politika, prosedür, talimat ve formların geliştirilmesi, KVKK ile ilgili yönetilebilir bir sistem kurulması ve kurulan bu sistemin denetlenmesi ve gerekli iyileştirmelerin yapılması için Veri Sorumlusu sıfatı ile Yönetim Kurulu, Kişisel Verileri Koruma Komitesi ve Veri Sorumlusu İrtibat Kişisi atar.
3. Kişisel verilerin kurum tarafından hazırlanan KVKK Politika ve prosedürlerine uygun olarak korunmasından ilgili sürece müdahil olan tüm çalışanlar müteselsilen sorumludur.
4. Kişisel veriler organizasyonel, idari, teknik, teknolojik imkanlar ve uygulamalar ile korunmakta ve yapılan iç ve dış denetimlerle güvenlik sıkılaştırması düzenli olarak yapılmaktadır.
5. Bilgi güvenliği, kişisel veri güvenliğinin sağlanması için konusunda deneyimli, teknik tecrübesi olan uzmanlar istihdam edilir.
6. Kurum çalışanları, kişisel veriler, özel nitelikli kişisel veriler ve kişisel verilerin korunması; kişisel verilerin hukuka uygun olarak işlenmesi konusunda bilinçlendirme eğitimleri alırlar. KVKK/GDPR Komitesi, Veri Sorumlusu İrtibat Kişisi'ne KVKK ile ilgili teknik eğitimler verilir.
7. Kurumda, kişisel verilere erişim yetkilendirilmiştir. Kişisel verilere erişmesi gereken çalışanların söz konusu kişisel verilere erişimini sağlamak adına gerekli KVKK prosedürleri işletilir, bu prosedürlerin oluşturulması ve uygulanmasından Veri Sorumlusu İrtibat Kişisi, KVKK/GDPR Komitesi müteselsilen sorumludur.
8. Kurum çalışanları, Kişisel verilere üzerinde yalnızca kendilerine tanımlanan yetki dâhilinde ve ilgili KVKK prosedürüne uygun olarak erişim sağlayabilir. Sehven dahi fazladan bir yetki açılmışsa bunu bildirmek çalışanın sorumluluğundadır. Eğer çalışan erişim yetkisini aşarsa, yapmış olduğu her türlü erişim ve işleme hukuka aykırı olup iş akdinin haklı nedenle feshine sebep olur.
9. Kurum çalışanları, kişisel verilerin güvenliğinin ihlali; yetkisiz erişim, özel nitelikli kişisel verilerin ifşası veya kişisel verilerin güvenliğinin yeterince sağlanmadığı şüphesi oluşursa durumu derhal Bilgi Güvenliği Olay İhlal Formu aracılığı ile Veri Sorumlusu İrtibat Kişisi'ne bildirir. Her ihlal şüphesi ilgili görevliler aracılığı ile KVKK/GDPR Komitesi'ne iletilir.
10. Kişisel Verilerin alınması, işlenmesi, güvenliği, güncellenmesi, silinmesi, anonim hale getirilmesi gibi durumlara yönelik detaylı KVKK politika, prosedür, talimat ve formları KVKK Koordinatörü, Veri Sorumlusu İrtibat Kişisi ve Komite tarafından oluşturulur.
11. Kurum çalışanlarından kendisine kurum mobil cihazları tahsis edilen her çalışan, Ayrıcalıklı Haklar Tablosu'na alınır. Çalışanlar kendi kullanımına tahsis edilen mobil cihazlarının güvenliğinden kendileri sorumludur.
12. Kurum çalışanları kendi sorumluluk alanında yer alan fiziki dosyaların güvenliğinden kendileri sorumludur. Dosyalar Temiz Masa Temiz Ekran Politikası'na uygun olarak korunur.

13. Kurum çalışanları kişisel verilerin güvenliği için talep edilen veya ek olarak talep edilecek olan güvenlik önlemleri olması durumunda tüm çalışanlar ek güvenlik önlemlerine uymak ve bu güvenlik önlemlerinin sürekliliğini sağlamak ile yükümlüdür.
14. Kurum Kişisel Verilerin Korunması Kanunu'na uyum sağlayabilmek için veri güvenliği konusunda yazılım ve teknolojik önlemleri alır. Firewall, antivirüs programı, Loglama, SIEM çözümleri, UTM, Sandbox, HoneyPot, DLP, Veri Maskeleme, Kriptolama, gibi çözümleri kurum bütçesine ve önceliğine uygun olarak hayata geçirir. Penetrasyon testleri gerçekleştirilir.
15. Kurumda iş sürekliliği esastır. Verilerin, kişisel verilerin kaybolmasını zarar görmesini, bütünlüğünün bozulmasını engellemek üzere yedekleme programları kullanılmakta ve yeterli düzeyde güvenlik önlemleri alınmaktadır. Kurum gerekli hallerde kullanmak üzere felaket kurtarma (disaster recovery) senaryolarına uygun olarak iş ve eylemler gerçekleştirecektir.
16. Kurumda, kişisel verilerin yer aldığı belgeler dijital ortamda ve fiziksel ortamlarda korunmaktadır. Bu kapsamda, kişisel veriler ortak alanlarda ve masaüstünde saklanmaz. Kişisel Verilerin yer aldığı dosya ve klasörler vb. belgeler masaüstüne veya ortak klasöre taşınmaz, KVKK/GDPR Komitesi, Veri Sorumlusu İrtibat Kişisi ve ilgili bilgi işlem yöneticisinin önceden yazılı onayı alınmadan Kurum bilgisayarlarındaki bilgiler USB vb. başka bir aygıta aktarılamaz, Kurum dışına çıkartılamaz.
17. KVKK/GDPR Komitesi, kurum içerisinde bulunan tüm kişisel verilerin korunmasına yönelik teknik ve idari önlemleri almak, gelişmeleri ve idari faaliyetleri sürekli takip etmekle ve gerekli KVKK politika, prosedür, talimat ve formları hazırlayarak Yönetim Kurulu onayına sunmak, onay akabinde Kurum içerisinde duyurmak ve bunlara uyulmasını sağlamak ve denetlemekle yükümlüdür. Bu kapsamda, Komite ve Veri Sorumlusu İrtibat Kişisi çalışanların farkındalığını artırmak üzere gerekli eğitimlerin düzenlenmesini sağlar.
18. Kurumda bir departman özel nitelikli kişisel veri işliyorsa, bu departman, Komite tarafından işledikleri kişisel verilerin önemi, güvenliği ve gizliliği hakkında bilgilendirilir ve ilgili departman Komite talimatlarına uygun hareket ederler. Özel nitelikli kişisel verilere erişim yetkisi yalnızca sınırlı çalışanlara verilir ve bunların listesi ve takibi Komite tarafından yapılır.
19. Kurum içerisinde işlenen özel nitelikli kişisel verilerin tamamı **"Gizli Bilgi"** olarak kabul edilir. Özel nitelikli kişisel veriler kâğıt üzerindeyse dosyanın ilk sayfasına beyaz A4 üzerine kırmızı renkte çerçeve içine alınmış bir şekilde hazırlanan kasede şu ibare yer alır:
"KVKK/GDPR Kişisel Veri/Özel Nitelikli Kişisel Veri GİZLİDİR"
20. Kurum çalışanları, Kişisel Verilerin güvenliğine ve gizliliğine ilişkin yükümlülüklerinin, iş ilişkisinin sona ermesinden sonra da devam edeceği konusunda bilgilendirilmiş ve Kurum çalışanlarından bu kurallara uymaları yönünde taahhüt alınmıştır.
21. Kurumda kişisel verilerin güvenliği konusunda güvenlik sıkılaştırması uygulanır. Her yıl kurum KVKK/GDPR ile ilgili uyumu sağlamak için üçüncü bir göz tarafından denetlenir ve bir denetim raporu hazırlanır. Bu rapor KVKK/GDPR Komitesi'ne iletilir. KVKK/GDPR Komitesi KVKK üçüncü göz denetim raporunu üst yönetime sunar.
22. Her yıl KVKK/GDPR kişisel veri güvenliği iç tetkiklerinde KVKK ile ilgili sorular denetimlerde sorulmak üzere ayrı bir liste halinde iç tetkikçilere verilir. İç tetkikçiler tetkik öncesinde yapılan eğitimlerde KVKK ile ilgili bilgilendirme yapılır.
23. Yapılan iç tetkiklerde ortaya çıkan KVKK uygunsuzlukları KVKK/GDPR Komitesi ve Veri Sorumlusu İrtibat Kişisi'ne iletilir. Çıkan uygunsuzlukların giderilmesi sağlanır.
24. Kurum Kişisel Veri Güvenliği protokolü gereği veri işleyen sıfatına sahip kurumları denetleyebilir. Denetimde iç tetkikçiler, komite üyeleri, kurumun bilgi güvenliği danışmanı bulunabilir. Denetim sonuç raporu KVKK/GDPR Komitesi'ne sunulur.
25. Kurumda Kişisel Veri Güvenliği protokolü gereği veri işleyen sıfatına sahip kurumlarda uygunsuzluk tespit ederse derhal KVKK/GDPR Komitesi'ni toplantıya davet eder. Gerekli uykusuzluklara karşı aksiyon alınması sağlanır.
26. Kurumda bilgi güvenliği ve kişisel veri güvenliğini ihlal eden çalışanlar için kurumsal düzenlemeler, yönetmelikler, yasal mevzuatlara uygun olarak disiplin, soruşturma ve adli işlemlerin yapılması sağlar.
27. Veri Minimizasyonu için gerekli önlemler alınır, çalışanlar konu ile ilgili periyodik olarak yılda 2 kez e-posta ile uyarılır.
28. Çalışanlar bilgi güvenliği kuralları ve kişisel veri güvenliği yönetim sistemi kuralları ile ilgili yılda 2 kez e-posta üzerinden, duyuru panoları üzerinden uyarılır.

29. Çalışanlar bilgi güvenliği ve 6698 sayılı yasa ile ilgili kişisel veri güvenliği yönetim sistemi ile ilgili kuralları ve bu kuralların güncel hallerini takip etmekten sorumludurlar. Güncellenen dokümanlar ortak klasör olan "BGYS-KVYS" üzerinden ve/veya kurumsal web sayfası üzerinde veya duyuru panoları üzerinde olabilir.

SORUMLULUKLAR

KVKK/GDPR Komitesi: Kişisel Veri Yönetimi ve Güvenliği Politikası'nın geliştirilmesinden ve politikanın yayımlanmasından, güncellenmesinden ve yayılımının sağlanmasından sorumludur.
KVKK/GDPR Veri Sorumlusu İrtibat Kişisi: Dokümanın düzenlenmesi ve revize edilmesinden sorumludur. KVKK ile ilgili İç Tetkiklerde soruların hazırlanması ve İç Tetkikçilerin eğitilmesinden sorumludur.
İç Tetkikçiler: Kişisel verilerin korunması ile ilgili soruları iç denetim sırasında sorulmasından sorumludur.
Tüm Yöneticileri: İç tetkik sonuçlarının takibinden iyileştirilmesinden. Kişisel verilerin yasalara uygun olarak alınmasından, işlenmesinden, güncellenmesinden, korunmasından, gerektiğinde silinmesinden, yok edilmesinden sorumludur.
Çalışanları: Kişisel verilerin yasalara uygun olarak alınmasından, işlenmesinden, güncellenmesinden, korunmasından ve KVKK ile ilgili tüm kurumsal politikalara uygun iş yapmaktan ve davranmaktan sorumludur.