Hisar Okulları
Kişisel Verilerin Korunması Komitesi
Çalışma Yönergesi

Yönergenin Amacı ve Tanımlar

Madde 1: Bu yönergenin amacı

Hisar Okulları Kişisel Verilerin Korunması Komitesi'ni oluşturmak ve çalışma yöntemini belirlemektir.

Madde 2: Tanımlar

A. 6698 Sayılı Kanun: 24.03.2016 tarihli Resmi Gazete'de yayınlanan Kişisel Verileri Koruma Kanunu,
B. Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi,
C. Anonim hale getirmek: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

Komitenin Amacı, Oluşturulması ve Yapısı

Madde 3: Komitenin amacı

Aşağıdaki konularda ilgili taraflarla işbirliği içinde çalışmalar yürütmek, Genel Müdür ve İcra Kuruluna iletilmek üzere öneriler geliştirmektir.

A. Kurum içinde veri gizliliğinin anlaşılmasını sağlamak ve riskleri belirlemek,
B. Veri gizliliği politika ve standartlarını tanımlamak ve güncel tutmak,
C. Politika, süreç ve prosedürlerini hazırlamak ve güncel tutmak,
D. Projeler kapsamında oluşabilecek risklere yönelik değerlendirmeleri gerçekleştirmek,
E. Belirlenen önlemlere yönelik aksiyonları almak ve süreçlere ilişkin kontrolleri tasarlamak,
F. Uygulanan yeni sistemlere yönelik güvenlik kontrollerinin teminatını sağlamak,
G. Güvenliğe ilişkin aktivitelerin ve çalışmaların izlenmesi ve kurulan güvenlik mekanizmalarının aktif işletilmesini sağlamak,
H. Kişisel verilerin ifşa edilmesine yönelik gerçekleşen olayların kayıt altına almak ve raporlamak,

I. Başvuru, şikayetler ve veri sorumluları sicili ile ilgili tanımları, takipleri ve raporlamaları yapmak,
J. Kişisel verilerin korunması kapsamında yaşanabilecek öngörülebilen vakalar ile ilgili bilinçlendirme eğitimi düzenlemek.

Madde 4: Komitenin Kurulması

A. Komite üyeleri ve Komite Başkanı, Genel Müdür tarafından 3 yıl görev yapacak şekilde aşağıdaki bölümlerden seçilir.
    a. Kurum İçi
        i. Bilgi İşlem Bölümü
        ii. Milli Eğitim ve/veya Öğrenci İşleri
        iii. İnsan Kaynakları
        iv. Müdür Yardımcısı
    b. Kurum Dışı
        i. Danışmanlık alınan hukuk firması

B. Komite her akademik yılda en az 2 kere toplanır ve toplantı sonucu oluşan raporu İcra Kurulu'na iletir.
C. Başkanın görev ve sorumlulukları aşağıdakileri içerir, ancak bunlarla sınırlı değildir; Başkan;
    a. Komitenin düzgün çalıştığından, tüm konuların tartışıldığından, etkili kararların alındığından ve bu kararların uygulandığından emin olur.
    b. Komite üyelerinin yükümlülüklerinin farkında olduğundan ve komitenin sorumluluklarına uyduğundan emin olacak şekilde liderlik eder.
    c. Herhangi bir konudak anlaşmazlık veya fikir ayrılıklarını çözmek için problem çözme becerilerini kullanır.
    d. Komite gündemleri ve eylemleri ile ilgili olarak Genel Müdür ve İcra Kurulu'nu bilgilendirir.
    e. Genel Müdür ve İcra Kurulu ile etkin iletişim ve koordinasyonu sağlar.
    f. Toplantıları düzenler ve yönetir. Toplantıları davetlerinin ve düzenlemelerinin kanunlara, okulun tüzük ve hükümlerine uygun olduğundan emin olur.
    g. Toplantıların profesyonel ve verimli bir ortamda düzenlendiğinden emin olur.
    h. Olağanüstü durumlarlada yetkin kriz yönetimi uygular, Genel Müdür ve İcra Kurulu'nu bilgilendirir.

Madde 5: Yöntem ve Prosedürler

A. Komitenin görev ve sorumlulukları aşağıda Ek 1'deki tabloda gösterilmiştir.
B. Süreçler ve yaşam döngüsü ile ilgili sorumluluklar Ek 2'deki tabloda gösterilmiştir.

Madde 6: Bilgilendirme ve Karar

A. Komite, Ek 1 ve Ek 2'de yer alan görevler ile ilgili olarak çalışmaları gerçekleştirir ve çalışmaların sonucu hakkında Genel Müdür ve İcra Kurulu'nu bilgilendirir.

B. KVK konusunda karar alınması ve eyleme geçilmesinin gerekli olduğu durumlarda Komite tarafından geliştirilen öneriler, karar alınmak üzere Genel Müdür ve İcra Kurulu'na iletilir.
C. Komite çalışmaları sırasında aşağıdaki belgelerden yararlanır ve gerektiğinde bu belgeleri güncelleyerek İcra Kurulu'na sunar.
    a. Aydınlatma yazısı,
    b. Kişisel Veri İşleme Envanteri ve Veri Sınıflandırma Prosedürü,
    c. Verilerin İşlenmesi ve Korunması Politikası,
    d. Veri Saklama ve İmha Politikası,
    e. Şikayet Başvuru ve İhlal Yönetimi Prosedürü,
    f. Kişisel Veri İhlal Olayı Bildirim Formu,
    g. Kişisel Veri İmha Formu,
    h. İlgili Kişi Başvuru Formu
D. Genel Müdür karar ve uygulamalar hakkında Kurucu Temsilcisine aylık bilgi verir

Yürürlük ve Yürütme

Madde 7: Bu yönerge Hisar Eğitim Vakfı Yönetim Kurulu onayı ile yürürlüğe girer.

Madde 8: Yönerge hükümlerini Genel Müdür yürütür. Genel Müdür yönergede ifade edilen tüm hükümlerde Kurucu Temsilcisine karşı sorumludur.

Ek 1: Görev ve Sorumluluk Alanları

Kişisel Verilerin Korunması Komitesi Görev ve Sorumluluk Alanları	OKUL YÖNETİMİ	KOMİTE BAŞKANI	KOMİTE ÜYELERİ	İLGİLİ UZMAN	UYUM / HUKUK
A. Veri Gizliliğinin Anlaşılması & Risklerin Belirlenmesi					
Hisar Okulları veri yönetim sistemi kapsamında değerlendirilecek olan risk toleranslarının anlaşılması ve tanımlanması	I	A	R	C	C
Hisar Okulları süreçlerine yönelik teknik ve idari güvenlik gereksinimlerinin tanımlanması	I	A	R	C	
Kişisel verilerin korunması kapsamında oluşabilecek risklerin yasal etkilerinin tanımlanması	I	A	R		C
Kişisel veri ifşa olaylarının önlenmesine yönelik kurulan teknik ve idari güvenlik ortamının işletilmesi	I	A	R	C	
B. Veri Gizliliği Politika ve Standartlarının Tanımlanması ve Güncel Tutulması					
Veri yönetim sistemi kapsamında politika, prosedür ve yardım dokümanlar tanımlanması ve onaylanması	I	A	R	C	C
Hisar Okulları süreçlerinde oluşan değişiklikler veya yeni bir sürece yönelik politika, prosedür ve yardımcı dokümanların güncellenmesi	I	A	R		
Politika, prosedür ve yardımcı dokümanların efektif bir kanal aracılığı ile tüm çalışanlara ve 3. taraflara duyurulması		A	R		
C. Standart Önlemlerin Belirlenmesi					
Belirlenen risk toleransı ile ilişkili, risklerin önlenmesi hususunda gerçekleştirilen çalışmaların, Hisar Okulları süreçleri ve stratejileri ile uyumlu olarak dokümante edilmesi	I	A	R	C	
Teknik ve idari güvenlik stratejilerinin BT, İş birimi yöneticileri ve üst yönetimin desteği ile hazırlanması		I	A	C	
Veri yönetim sistemi kapsamında karşılaşılan risklerin giderilmesine yönelik aksiyonların belirlenmesi (riskin kabul edilmesi, riskten kaçınılması, riske yönelik hafifletici önlemlerin alınması, riskin transfer edilmesi)		A	R	C	
Sektörde iyi uygulama olarak tanımlanan süreçlerin ve teknolojilerin takip edilmesi, kişisel verilerin korunması kapsamında faydalarının çalışılması		A	R	C	
Kişisel verilerin korunmasına yönelik teknik ve idari güvenlik tedbirleri bütçe ve planlama çalışmalarının gerçekleştirilmesi	I	A	R	C	

D. Projeler Kapsamında Oluşabilecek Risklere Yönelik Değerlendirmelerin Gerçekleştirilmesi					
Hisar Okulları genelinde gerçekleştirilen projelere yönelik risk değerlendirmelerinin Kişisel Verilerin Korunması Kanunu açısından değerlendirilmesi ve uyuma yönelik standart yaklaşımların belirlenmesi		I	A	C	C
Gerçekleştirilen projeler esnasında kişisel verilerin korunması açısından gerçekleştirilen risk değerlendirmelerine yönelik eğitim aktivitelerinin gerçekleştirilmesi		A	R		
E. Belirlenen Önlemlere Yönelik Aksiyonların Alınması ve Süreçlere İlişkin Kontrollerin Tasarımı					
Kişisel verilerin korunması kapsamında oluşturulan risk değerlendirme çıktılarına yönelik alınması gereken aksiyonların standartlaştırılması		A	R		
Uygun standart önlemlerin belirlenemediği durumlarda gerçekleştirilen aktivitelere yönelik yeni aksiyonların belirlenmesi, risk yaklaşımlarının gözden geçirilmesi		A	R	C	
Risklerin ilerleyen süreçte oluşturacağı etkilerini azaltmaya yönelik stratejilerin belirlenmesi		A	R	C	C
Tanımlanan yeni prosedürlerin üst yönetime raporlanmasına ilişkin kontrol aktivitelerinin belirlenmesi	I	A	R		
F. Uygulanan Yeni Sistemlere Yönelik Güvenlik Kontrollerinin Teminatının Sağlanması					
Teknik ve idari güvenlik kontrollerine yönelik uygun test seviyelerinin belirlenmesi adına risk tiplerinin tanımlanması (düşük, orta, yüksek)		A	R	C	C
Teknik ve idari güvenlik kontrolleri ve gerçekleştirilen aktivitelerin stratejik hedefler ile uygunluğunun kontrol edilmesi	I	A	R		
Uygulanan yeni sistemlere yönelik veri yönetim sistemi dahilinde oluşturulan politikaları, prosedürleri ve yardımcı dokümanları ihlal edecek durumların belirlenmesi ve kabul edilmesine yönelik kararların alınması	I	A	R		
Uygulanan yeni sistemlere yönelik siber tehditlerin belirlenmesi ve raporlanması	I	R	R	A	
Sistemler üzerinde kişisel verilerin korunması kapsamında denetim izi ayarlarının aktif edilmesi		R	R	A	
G. Güvenliğe İlişkin Aktivitelerin ve Çalışmaların İzlenmesi ve Kurulan Güvenlik Mekanizmalarının Aktif İşletilmesinin Sağlanması					
Teknik ve idari güvenlik kontrolleri operasyonlarına yönelik ana hatların belirlenmesi		R	R	A	
Teknik güvenlik kontrollerine yönelik oluşabilecek zafiyet ve tehditlerin aktif olarak izlenmesi ve raporlanması		I	R	A	
Mevcut altyapı kapsamında operasyonel tehditlerin ve gereksinimlerin belirlenmesine yönelik farkındalık aktivitelerinin gerçekleştirilmesi		A	R	R	
Altyapı sürekliliğine yönelik gereksinimlerin belirlenmesi ve mevcut altyapının sürekliliğinin sağlanması kapsamında çalışmaların gerçekleştirilmesi		I	R	A	
Gerekli güvenlik araçlarının kullanımının teşvik edilmesi		R	R	C	
H. Kişisel Verilerin İfşa Edilmesine Yönelik Gerçekleşen Olayların Kayıt Altına Alınması ve Raporlanması					
Kişisel veri ifşa olaylarının bildirilmesine yönelik iletişim kanallarının operasyonel etkinliğinin sağlanması		R	A	C	

I. Başvuru, Şikayet ve Veri Sorumluları Sicili					
İlgili kişi tarafından gerçekleştirilen başvurular veya yapılan şikayetlere ilişkin iletişim kanallarının tanımlanması		A	R	C	
Başvurulara ve şikayetlere ilişkin yapılan taleplerin sonuçlandırılmasına yönelik kanun hükmünde belirtilen cevap süresinin takip edilmesi		A	R		
Başvurulara ve şikayetlere ilişkin periyodik raporlamaların yapılması		I	R	C	
J. Kişisel Verilerin Korunması Kapsamında Yaşanan Olaylardan Ders Çıkarılması ve Eğitimlerin Düzenlenmesi					
Kişisel verilerin korunmasına yönelik tüm çalışanların farkındalığının arttırılması ve sorumlulukların aktarılması adına eğitimlerin düzenlenmesi		A	R	C	C
Kişisel verilerin korunmasına yönelik belirlenen stratejilere yönelik çalışanların bilgilendirilmesi		A	R		

Ek 2: Yaşam Döngüsü Adımları

Kişisel Verilerin Korunması Yaşam Döngüsü Adımları ve Atanan Görevler	OKUL YÖNETİMİ	KVKK KOMİTESİ	TÜM ÇALIŞANLAR	İLGİLİ UZMAN	UYUM / HUKUK
A. Veri Gizliliğinin Anlaşılması & Risklerin Belirlenmesi					
Hisar Okulları'nın stratejik yönelimi doğrultusunda, kişisel veri gizliliğinin gerçekleştirilen süreçlerine etkisinin tanımlanması	A	R			
Kişisel verilerin korunmasına yönelik kritik risklerin belirlenmesi ve Hisar Okulları üzerinde oluşturacağı etkilerin değerlendirilmesi	A	R			
Veri yönetim sisteminin sürdürülebilirliğinin sağlanması adına iş birimlerinin katılımını sağlamak ve ilgili tarafların sorumlu oldukları yönetim sistemi kontrollerini tanımlamak	A	R		C	
Veri yönetim sistemi dahilinde birden fazla iş sürecini etkileyecek olan risklerin tanımlanması	I	A		C	
Veri yönetim sistemine yönelik risklerin belirlenmesi, risk sahiplerine iletilmesi ve alınan aksiyonların takibi gibi ilgili birimler tarafından işletilen süreçlerin aktif takip edilmesi	R	A			
Veri gizliliğini önlemeye yönelik gerekli teknik ve idari önlemlerin güncel teknolojilerle ve süreçlerle desteklenmesi	I	R		A	
Veri gizliliği kapsamında oluşturulan teknik ve idari güvenlik ortamının denetlenmesi ve ilgili raporların üst yönetime iletilmesi	I	A		R	R
B. Veri Güvenliği Politika ve Standartlarının Tanımlanması ve Güncel Tutulması					
Veri yönetim sistemi kapsamında politika, prosedür ve yardım dokümanlar tanımlanması ve onaylanması	A	R			
Hisar Okulları süreçlerinde oluşan değişiklikler veya yeni bir sürece yönelik politika, prosedür ve yardımcı dokümanların güncellenmesi	I	A		R	R
C. Güvenliğe İlişkin Aktivitelerin ve Çalışmaların İzlenmesi ve Kurulan Güvenlik Mekanizmalarının Aktif İşletilmesinin Sağlanması					
Veri güvenliğine ilişkin alınan teknik ve idari tedbirler kapsamında kurulan güvenlik araçlarının kullanılması ve fonksiyonaliteye yönelik değerlendirmelerin gerçekleştirilmesi	I	C	R	R	
D. Kişisel Verilerin İfşa Edilmesine Yönelik Gerçekleşen Olayların Kayıt Altına Alınması ve Raporlanması					
Kişisel verilerin ifşa olmasına yönelik gerçekleşen olaylara ilişkin kayıtların	I	A	R	C	C

oluşturulması ve Komite'ye raporlanması					
Kişisel verilerin ifşa olmasına yönelik şüpheli durumların Komite'ye raporlanması		I	A	C	C
E. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonimleştirilmesi					
Kişisel verilere yönelik tanımlanan imha sürelerinin takip edilmesi		A	R		
Kişisel veri içeren imha edilecek varlıkların uygun şartlar altında silinmesi, yok edilmesi veya anonimleştirilmesinin sağlanması		I	R	C	
İmha gerçekleştirilen kişisel verilere yönelik imha kayıtlarının oluşturulması ve saklanması		A	R	C	