# ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ, ISO/IEC 27701 STANDARDI VE KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA DANIŞMANLIK HİZMETİ İŞİ TEKNİK ŞARTNAMESİ

2023, T.C. Hakkâri Üniversitesi, Bilgi İşlem Daire Başkanlığı

# İÇİNDEKİLER

# 1. TANIMLAMALAR VE KISALTMALAR

| | | | |
|---|---|---|---|
| **1.1.** | **Üniversite** | : | T.C. Hakkari Üniversitesi |
| **1.2.** | **İdare** | : | T.C. Hakkari Üniversitesi, Bilgi İşlem Daire Başkanlığı |
| **1.3.** | **İstekli** | : | Teklif veren gerçek veya tüzel kişi/kişiler |
| **1.4.** | **Yüklenici** | : | İşi alan gerçek veya tüzel kişi/kişiler |
| **1.5.** | **Kurul** | : | Kişisel Verileri Koruma Kurulu |
| **1.6.** | **Kurum** | : | Kişisel Verileri Koruma Kurumu |
| **1.7.** | **İş** | : | ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti |
| **1.8.** | **ISO27001** | : | ISO 27001 Bilgi Güvenliği Yönetim Sistemi |
| **1.9.** | **ISO/IEC 27701** | : | ISO 27001 Bilgi Güvenliği Yönetimi ve ISO/IEC 27002 Güvenlik Denetimleri standartlarının kapsamını genişleten bir eklenti |
| **1.10.** | **KVKK** | : | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| **1.11.** | **BT** | : | Bilgi Teknolojileri |
| **1.12.** | **BYT** | : | Bilgi Yönetim Sistemi |
| **1.13.** | **İdare Proje Ekibi** | : | ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti işini yönetecek ve yükleniciye destek sağlayacak, idare tarafından oluşturulan ekip |
| **1.14.** | **Yüklenici Proje Ekibi** | : | ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti işini yürütecek, yüklenici tarafından oluşturulan ekip |
| **1.15.** | **Veri Sorumlusu** | : | Üniversitenin kendisidir. |
| **1.16.** | **Veri Sorumlusu Yöneticisi** | : | Üniversitemizi temsile yetkili Rektörlük Makamınca, Kanunun uygulanması bakımından yerine getirilecek yükümlülükler ile ilgili olarak Veri Sorumlusu Yöneticisi olarak atanmış kişi |
| **1.17.** | **İrtibat Kişisi** | : | Veri Sorumlusu Yöneticisi tarafından https://verbis.kvkk.gov.tr/User/DRLogin adresinden tanımlanan, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen kişi |
| **1.18.** | **GDRP** | : | Genel Veri Koruma Yönetmeliği (General Data Protection Regulation) |
| **1.19.** | **Açık Rıza** | : | Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür irade ile açıklanan rızayı |

| | | | |
|---|---|---|---|
| **1.20.** | **Veri Kayıt Sistemi** | : | Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi |
| **1.21.** | **Proses** | : | Olguların ya da olayların belli bir taslağa uygun ve belli bir sonuca varacak biçimde düzenlenmesi ve art arda sıralanması. Bir şeyin yapılış, üretiliş biçimini oluşturan sürekli işlemler, eylemler dizisi, süreç. |
| **1.22.** | **Politika** | : | İdare'nin etkinliklerini amaç, yöntem ve içerik olarak düzenleme ve gerçekleştirme esaslarının bütünü. |
| **1.23.** | **Yönerge** | : | Düzeni sağlamak için hazırlanan kuralların yazılı olduğu belge |
| **1.24.** | **Prosedür** | : | Bir amaca ulaşmak için tutulan yol ve yöntem (metot). Proses düzeyinde yapılan işlerin tüm detaylarını (yol, yöntem, sorumluluk, formlar) adım adım anlatan doküman |
| **1.25.** | **Form** | : | Bir şeyin istenilen ve olması gereken durumu; İstenilen şeylerin yazılması, doldurulması için hazırlanmış basılı belge. |
| **1.26.** | **Talimat** | : | Operasyonel düzeydeki uygulamaların tarif edildiği doküman |
| **1.27.** | **SWOT** | : | Güçlü yönler, Zayıf yönler, Fırsatlar, Tehditler (Strengths, Weaknesses, Opportunities, Threats) |

## 2. AMAÇ

**2.1.** Bu şartname ile İdare bünyesinde KVKK, ISO 27001 ve ISO/IEC 27701 sırasıyla kanun, belge ve standardı için gereksinimlerin belirlenmesi, belirlenen gereksinimlere göre yapılması gereken faaliyetlerin tanımlanması ve gereği hususunda dokümante edilmesi amaçlanmaktadır.

## 3. KAPSAM

**3.1.** KVKK, ISO 27001 ve ISO/IEC 27701 sırasıyla kanun, belge ve standardı için gereksinimlerin uygulanması niteliğinde; mevcut durum değerlendirmesi ve raporlanması, kapsam dahili tüm süreçler temelinde bilgi varlık envanterinin hazırlanması, varlık temelli risk değerlendirmesi ve işlenmesi için rehberlik yapılması, güvenlik önlemlerinin ve alınacak aksiyonların tespit edilmesi, ilgili kanun, belge ve standart gerekliliği ve İdare ihtiyacına özel tüm proses, politika, prosedür, talimat, yönerge ve form türünde dokümanların oluşturulması, rehberlik edilmesi, iç denetimin varsa Kurum içi sertifikalı İç Denetçiler ile birlikte gerçekleştirilmesi ve raporlanması, bilgi güvenliği yönetim sistemi uygulama ve bilgi güvenliği farkındalık eğitimlerinin kapsam dahili çalışanlara verilmesini kapsamaktadır.

**3.2.** ISO 27001 ve ISO/IEC 27701 denetimi öncesinde İdare'deki tüm eksikliklerin tamamlanması, ISO 27001'in ve ISO/IEC 27701'in gerekli kıldığı bilgi güvenliği denetimlerinin gerçekleştirilmesi, sertifika kuruluşunun gerçek denetimi için tüm şartların uygun hale getirilerek belgenin alınma sürecine danışmanlık edilmesini kapsamaktadır. Ayrıca sertifika kuruluşu tarafından gerçekleştirilecek denetim sonrasında ortaya çıkabilecek bulguların giderilmesi de kapsam dahilinde yürütülecek çalışmalar arasına alınmalıdır.

## 4. YÜKLENİCİ VE/VEYA İSTEKLİ YETERLİLİĞİ

**4.1.** Bu şartname kapsamında belirtilen hizmetleri kapsayan projeye benzer (Yönetim Sistemi Projesi, KVKK Projesi, Entegre Sistem Projesi ... vb) en az 5 (beş) adet diğer kurum ve kuruluşlarda gerçekleştirilmiş, belgelendirilmiş referansa sahip olmalıdır.

4.1.1. Bu beş kurum/kuruluştan en az ikisinin çalışan sayısının 50'ün üzerinde olması gerekmektedir.

**4.2.** GPDR hakkında bilgi sahibi olmalı ve bu kapsamında uyum çalışmalarını sağlayabilmelidir.

**4.3.** Yüklenici tarafından hizmet sağlamak ile yükümlü olacak yüklenici proje ekibi üyelerinden en az 1 (bir) tanesi ISO 27001 gerekliliklerini iyi derecede bildiğini göstermesi adına ISO 27001 Baş Denetçi Sertifikasına sahip olması gerekmektedir.

**4.4.** Yüklenici tarafından hizmet sağlamak ile yükümlü olacak yüklenici proje ekibi üyelerinden en az 1 (bir) tanesi ISO 27001:2013 standardı EK A 17.1 maddesinde özellikle açıklanan ve kurumumuzca da önem verilen iş sürekliliği gerekliliklerini iyi derecede bilmesi gerekmektedir.

**4.5.** Yüklenici, yüklenici proje ekibinden 1 (bir) personelini Proje Yöneticisi olarak atamak, ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti işindeki tüm süreçlerde İdare'nin muhatap kabul edebileceği, sorumlu tek isim olarak bildirmekle yükümlüdür.

**4.6.** Yüklenici proje ekibine yönetici olarak atanacak kişi, daha önce benzer iş tecrübesine sahip olmalıdır.

**4.7.** Yüklenici, yüklenici proje ekibinde yer alacak kişilerin; özgeçmişini, iş deneyimini, sahip olduğu sertifikaları ve benzer işlerde çalıştığına dair özel sektör, kurum ve/veya kuruluştan alınan hizmet sürelerini ve deneyimlerini gösteren hizmet dökümü belgelerini ( kamu ve/veya özel sektörde yukarıdaki deneyimlerini gösterir kamu ve/veya özel sektör kurum ve/veya kuruluşlarınca onaylanmış resmi nitelikteki referans dokümanını/belgesini) teklifinde İdare'ye sunmalıdır.

## 5. TEKLİF VEREMEYECEK OLANLAR (İSTEKLİ OLAMAYACAKLAR)

**5.1.** Aşağıda yazılı gerçek yada tüzel kişi/kişiler, doğrudan doğruya veya dolaylı olarak teklif veremezler, teklif vermiş olsalar dahi tespiti halinde teklifleri dikkate alınmaz ve satın alma kararı alınmışsa iptal edilir.

5.1.1. İdare Yönetim Kurulunda ve/veya İdare Denetim Kurulunda görev alan üyeler

5.1.2. İdare personeli

5.1.3. İdareden ayrılan personel ile İdare Yönetim ve Denetim Kurulu üyeliğinden ayrılmış bulunanlar, ayrıldıkları tarihten itibaren üç yıl müddetle

5.1.4. Bu fıkranın (1) ve (2) ve (3) bentlerinde sayılanların ortak olduğu tüzel kişilikler

5.2. Kamu ihalelerine katılmaları muhtelif kanunlarla yasaklanmış olanlar

## 6. GENEL KOŞULLAR

**6.1. Hizmetin gizliliği;** Yüklenici şartnamede tanımlanan hizmet aşamalarına ait işlerle ilgili hiçbir bilgiyi idareden saklamayacak, idare tarafından belirlenen idare proje ekibindeki personele tüm bilgileri istenildiği zaman verecektir. İdare ortamında öğrenilen tüm bilgiler ÇOK GİZLİ statüsünde olup yüklenici, idare ile ilgili öğrendiği hiçbir bilgiyi hizmet süresince ve sözleşme süresi sonrasında üçüncü şahıslar ile paylaşmayacağını taahhüt edecektir. Bu hizmet kapsamında çalışacak bütün personel ile hizmet başlamadan önce **EK – I Gizlilik Taahhütnamesi** imzalanması istenecektir. Türk yargı mercilerinin kararları saklı kalmak kaydıyla sözleşmenin amaçları doğrultusunda herhangi bir ifşa veya yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa, idarenin bu konudaki kararı nihai olacaktır. Gizlilik yükümlülüğü, işbu işe ait sözleşmenin herhangi bir nedenle sona ermesinden sonra da devam eder. Yüklenici, sözleşmenin imzalanmasına müteakip gizlilik taahhütnamesini imzalayarak idareye sunacaktır.

**6.2.** Yüklenici, yüklenici proje ekibinin kim olduğunu, ekip çalışanlarının mesai içi ve mesai dışı saatlerde ulaşılabilecek telefon numaralarını, e-posta adreslerini, idareye yazılı olarak sözleşme sırasında sunacaktır.

**6.3.** Oluşturulacak proses, prosedür, politika, form ve/veya yönerge gibi dokümanlarda yer alacak hükümler; tereddüde, yanlış anlamaya ve bir isteğin diğeri ile çelişmesine imkân bırakmayacak şekilde, açık ve kesin olmalı, ilgili tüm mevzuatlar hükümlerince hazırlanmalıdır.

**6.4. Ön Hazırlık:** Yüklenici tarafından İdare organizasyonunun incelemeleri yapılacak, varsa mevcut politika, BT süreç akışları, prosedür, talimat, form, yönetmelik ve yönerge gibi dokümanlar incelenecektir. Yüklenici, ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti işi kapsamında izleyeceği metot ve yöntemleri, iş adımları, örnek iş çıktıları, yüklenici proje ekibi, iş faaliyetleri, efor bilgisi ile iş takvimi bilgilerini içeren ayrıntılı bir iş planını hazırlayıp idareye sunmalıdır. Sunulan iş planı üzerinde İdare ve Yüklenici karşılıklı olarak anlaştıktan sonra iş başlatılacaktır.

**6.5.** Yüklenici, işe ait çalışmaları, İdare lokasyonunda gerçekleştirebileceği gibi, uzaktan bağlantı ile de yürütebilir. Ancak ön hazırlık aşamasında en az 1 (bir) kez ve

iş takvimi boyunca en az 2 (iki) kez olmak üzere toplamda en az 3 (üç) kez İdare lokasyonunda yüklenici proje ekibinin bulunması gerekmektedir.

**6.6.** Sözleşme yapılmasından sonra yüklenici proje ekibi değişikliği gibi durumlarda; yukarıdaki ilgili maddelerde belirtilen benzer özelliklere ve deneyimlere sahip olmaları durumunda, yüklenici proje ekibi değişikliği İdarece kabul edilebilecektir. İş planı, iş paylaşımı, vb. alanlardaki değişiklikler ise İdare'ye danışılacak, İdare'nin kabul ettiği hallerde uygulanacaktır.

**6.7.** Yüklenici, haftalık ilerlemeleri bir plan dâhilinde İdare'ye iletmeli ve söz konusu planda görevlendirmeler ile sorumluluk dağılımlarını net olarak belirtmelidir. Yüklenici, kendi proje ekibinin sorumluklarını yerine getirdiğinden emin olmalıdır. İş takviminde Yüklenici kaynaklı gecikme yaşanmamalıdır. İdare kaynaklı gecikmeler ise raporlanacak ve nasıl ilerleneceği bu raporlar doğrultusunda karara bağlanacaktır.

**6.8.** Yüklenici tarafından, işin başlangıcında sunulacak iş planı çerçevesinde tamamlanan her aşama için İdare' ye ilerleme raporu sunulacaktır.

**6.9.** Yüklenici ISO 27001 ve ISO 27701 denetimi öncesinde İdare'deki tüm eksiklikleri tamamlamış, bir final provası niteliğinde standartların gerekli kıldığı güvenlik denetimlerini gerçekleştirmiş ve belgelendirme kuruluşunun gerçek denetimi için tüm şartları uygun hale getirmiş olmalıdır.

**6.10. İşin Süresi;** sözleşme imzalanmasından itibaren 120 (yüz yirmi) takvim günüdür.

**6.11.** Yüklenici, İdare'nin tercih edeceği bir Sertifikasyon kuruluşuna başvuru yapılması ve belge alınması konusunda rehberlik etmelidir.

**6.12.** Sertifikasyon denetimi sonrası Sertifikasyon Kuruluşu tarafından tespit edilen açıklıklar İdare ile birlikte çalışılarak Yüklenici tarafından kapatılacaktır.

**6.13.** Yüklenici anılan işi teknik şartnamedeki hükümlere göre yerine getirmekle yükümlüdür. Aksi durumda uygunsuzluklar tespit edilip uyarıda bulunulur. Uygunsuzlukların devamı durumunda kendisine İdare tarafından hiçbir ödeme yapılmayarak uygunsuzluğun gidermesi talep edilir.

## 7. VERİLECEK HİZMETLERE AİT KOŞULLAR

### 7.1. Mevcut Durum Değerlendirmesi

7.1.1. İş kapsamında İdare'deki mevcut süreç ve uygulamalar incelenecek, dokümanlar gözden geçirilecektir. Mevcut durum değerlendirmesi sonucunda mevcut durumu gösteren bir rapor hazırlanacak ve işbu rapor ışığında detaylı bir

proje planı oluşturulacaktır. Raporda KVKK, ISO 27001 ve ISO/IEC 27701 sırasıyla kanun, belge ve standardı ana ve kontrol maddelerine uyum değerlendirilecektir.

7.1.2. KVKK, ISO 27001 ve ISO/IEC 27701 sırasıyla kanun, belge ve standardı ana ve kontrol maddelerine uyumun tam ya da hiç olmadığı durumlar için yapılması gereken iyileştirmeler hazırlanacak mevcut durumu gösteren raporda detaylı olarak belirtilecektir.

### 7.2. 6698 sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Yürütülecek Çalışmalar

7.2.1. Varlık ve bilgi envanteri oluşturulması sağlanmalıdır. Yüklenici, varlık ve bilgi değerlendirmesi yapacaktır. Bu kapsamda İdare'nin mevcut varlıkları ve bilgileri gözden geçirilecek İdare proje ekibi ile birlikte İdare içerisinde yer alan bilgi sahipleri ile görüşülüp tüm bilgiler ve varlıklar ortaya çıkarılacak, sahipleri ve ilişkili oldukları kaynaklar belirlenecek, bilgi güvenliği/varlık sınıflandırması, derecelendirmesi ve etiketlenmesi yapılarak, gizlilik, bütünlük, erişilebilirlik seviyeleri belirlenecektir.

7.2.2. KVKK ve bağıl yönetmelikleri kapsamında İdare'nin Veri İşleme süreçleri uyumlandırılacaktır.

7.2.3. KVKK ve bağıl yönetmelikleri kapsamında İdare'nin Veri Aktarım süreçleri uyumlandırılacaktır.

7.2.4. Yüklenici tarafından KVKK ve bağıl yönetmelikleri kapsamında gerekli tüm prosedür, proses, talimat, politika, form ve/veya yönerge vb. dokümanlar İdare'de mevcut ise güncellenecek, mevcut değil ise KVKK ve bağıl yönetmelikleri kapsamında hazırlanacaktır.

7.2.5. Yüklenici, KVKK ve bağıl yönetmelikleri kapsamında, başvuru, şikayet, itiraz gibi süreçlerin oluşturulmasını / uyumlandırılmasını sağlayacaktır.

7.2.6. Yüklenici, KVKK ve bağıl yönetmelikleri kapsamında Açık Rıza ve Aydınlatma metinlerinin oluşturulmasını / uyumlandırılmasını sağlayacaktır.

7.2.7. Yüklenici, İdare tarafından kullanılan verilerin, KVKK ve bağıl yönetmeliklerin öngördüğü şekliyle imha edilmesi ve gerekli süreçlerin yönetilmesi için gerekli **dokümanların oluşturulmasını - uyumlandırılmasını** sağlayacaktır.

7.2.8. İdare içindeki tüm aktif cihazlar, kenar uç nokta cihazlar ve kişisel veri kullanılan uygulamalar nezdinde mahremiyet analizi, kişisel veri analizi, veri sınıflandırması ve etiketleme analizi, kişisel veri alanlarının erişim ve yetkilendirme analizinin gerçekleştirilmesi sağlanacaktır.

7.2.9. Yüklenici tarafından Swot analizi yapılacak, veri güvenliği için iç ve dış tehditler belirlenecektir.

7.2.10. Yüklenici tarafından İdare adına KVKK ve bağıl yönetmeliklerine uygun şekilde devlete beyan hususunda gerekli iş ve işlemler için yönlendirme ve danışmanlık sağlanacaktır.

7.2.11. KVKK ve bağıl yönetmelikleri kapsamında İdare tarafından nitelikli ve/veya öz nitelikli verilerin depolanma ortamlarında ve süreçlerinde uygulanacak kontroller ile ilgili işletim ve yönetim detayları hakkında gerekli görülen prosedür, proses, talimat, politika, form ve/veya yönerge oluşturulacaktır.

7.2.12. Yüklenici KVKK hakkında bilgilendirmeler yaparak farkındalığın arttırılması adına gerekli eğitimleri sağlayacaktır.

### 7.3. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kapsamında Yürütülecek Çalışmalar

7.3.1. İdare faaliyetlerinin ISO 27001 standartlarına uygun hale getirilmesi için yapılması gerekenler hususunda Yüklenici tarafından İdare'ye ait varlık ve bilgi envanteri değerlendirmesi yapılacak, değerlendirme sonucunda standardın gerektirdiği koşullarda doğru, nitelikli ve uygulanabilir düzenlemeler sağlanacak şekilde elektronik ortamda indekslenebilir ve sıralı şekilde kategorize edilmiş halde varlık ve bilgi envanter kaydı oluşturulacaktır.

7.3.2. Yüklenici tarafından İdare'nin mevcut bilgi güvenliği yönetim sistemi incelenecek, sistemin, ISO 27001 standardına uygun ve sürdürülebilir hale getirilmesi için kural ve esaslar belirlenecektir.

7.3.3. Yüklenici, ISO 27001 standartları kapsamında, risk yönetim faaliyetlerine rehberlik edecektir. İdare proje ekibi ve yüklenici proje ekibi İdare'ye ait faaliyetler ile ilgili risk değerlendirme yaklaşımı belirleyecek, varlıklara ait gizlilik, bütünlük ve erişilebilirlik açısından bilgi güvenliğini etkileyecek riskler ile sahipleri belirlenecektir. Risk metriksleri, ölçüm metotları, riskin etki ve olasılık değerleri tespit edilecektir. Risk analiz sonuçları, risk analiz

raporu yüklenici tarafından oluşturulup İdare'ye teslim edilecektir. Kabul edilebilir risk seviyesinin belirlenmesi İdare sorumluluğunda olacaktır.

7.3.4. Yüklenici ISO 27001 standardı kapsamında hazırlanması gereken prosedür, proses, talimat, politika, form ve/veya yönerge vb. dokümanları İdare'de mevcutta var ise güncelleyecek mevcut değil ise oluşturacaktır.

7.3.5. Yüklenici ISO 27001 denetlenmesi ve muhtemel bir belgelendirme için danışmanlık süreci ile buna bağıl olarak belgenin devamı için sözleşme süresince gözetim hizmetleri sağlayacaktır.

7.3.6. Yüklenici ISO 27001 hakkında bilgilendirmeler yaparak farkındalığın arttırılması adına gerekli eğitimleri sağlayacaktır.

7.3.7. Yüklenici, ISO 27001 standartları gereği İdare'nin;

7.3.7.1. Doğru, güvenilir ve geçerli bilgi sağlaması,

7.3.7.2. Fazladan iş yükü ve gereksiz zaman kaybının önüne geçilmesi,

7.3.7.3. Riskleri minimize etme

7.3.7.4. İş sürekliliği

7.3.7.5. Bilgi varlıklarının gizliliğinin korunması

7.3.7.6. İdare genelinde bilgi sistemleri ve zayıflıkların nasıl korunacağı konusundaki farkındalık

7.3.7.7. Yasal taraftan zorunlu kılınan kriterler

7.3.7.8. Bilgi varlıklarına erişim koruması hususlarında danışmanlık hizmeti sağlayacaktır.

### 7.4. ISO/IEC 27701 Standardı Kapsamında Yürütülecek Çalışmalar

7.4.1. Yüklenici bilgi güvenliği standardı ISO 27001 ile entegrasyonu sağlayacak şekilde İdare içinde karmaşıklığı engelleyecek tedbirlerin alınması hususunda danışmanlık hizmeti sağlayacaktır.

7.4.2. Yüklenici, İdare'nin hassas verilerini sistematik olarak yönetmesi için ihtiyaç duyacağı ve mevzuatlar gereği ihtiyaç olunan tüm prosedür, proses, talimat, politika, form ve/veya yönerge vb. dokümanları İdare'de mevcutta var ise güncelleyecek mevcut değil ise oluşturacaktır.

7.4.3. Yüklenici, İdare'nin KVKK, GDPR vb. ulusal ve uluslararası veri koruma kanun, yönetmelik ve mevzuatlarına uyumunu sağlayacaktır. Mevzuatlarda çakışma söz konusu olursa öncelik ulusal (KVKK gibi) kanun, yönetmelik ve mevzuatlar olacaktır.

7.4.4. Yüklenici, kişisel verilerin gizliliğinin yönetimi konusunda İdare'nin güvence sağlamasına danışmanlık edecektir.

7.4.5. Yüklenici, Gizliliğin yönetimine ilişkin mevzuatlarca gerekli tüm süreçlerin İdare için kurumsallaştırılmasına danışmanlık edecektir.

7.4.6. Yüklenici, Kişisel verilerin gizliliğinin ve veri koruma anlayışının İdarece içselleştirilmesine destek olacak, gerekli farkındalık eğitimlerini verecektir.

7.4.7. Yüklenici, İdare'nin ISO/IEC 27701 standartları gereği, güvenlik ihlallerinin etkisini proaktif olarak sınırlandırarak riskleri en aza indirmesi ve iş sürekliliğini sağlaması adına danışmanlık hizmeti sağlayacaktır

## 8. DOKÜMANTASYON ve RAPORLAMA

**8.1.** İşbu teknik şartnamede belirtilen hususlar yerine getirilirken sanal ortamda (soft-copy) oluşturulacak bir klasör içine aşağıda belirtilen ve/veya belirtilmeyip ihtiyacı öngörülen dokümanlar eklenecektir.

8.1.1. Tüm proje bilgileri,

8.1.2. Değerlendirme ve sonuç raporları,

8.1.3. Aydınlatma Metinleri,

8.1.4. Beyanlar,

8.1.5. Açık Rıza Sözleşmeleri,

8.1.6. Başvuru Formları ve Cevap Formları,

8.1.7. Veri Paylaşımı ve Veri Transferi Sözleşmeleri,

8.1.8. İmzalanacak sözleşmelerde dikkat edilecek hususlar ve eklenmesi gereken metinler, dikkat edilmesi gereken noktalar

8.1.9. İşbu şartname maddelerinde belirtilen hazırlanacak tüm prosedür, proses, form, talimat, politika, yönerge vb. dokümanlar

**8.2.** Tüm oluşturulacak dokümanlar için İdare onayı alınacak, onay verildikten sonra klasöre eklenecektir.

**8.3.** Bahse konu klasör İdare tarafından tahsis edilecek dijital ortamda İdare'ye teslim edilecektir. Ayrıca işbu dokümanlar Yüklenici imza ve kaşesi ile de elden (Hard-copy) teslim edilecektir.

# EK-I GİZLİLİK TAAHÜTNAMESİ

Bu taahhütname Hakkari Üniversitesi ile ..... firması arasındaki ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti iş ilişkisi sebebiyle oluşan/oluşacak her türlü Üniversitemize ait iş/işlemlerin, akademik ve idari personel ile öğrenciye ait verilerin, ..... firması tarafından elde edilecek veya üretilecek bilgiler ile kullanacakları bilgi varlıklarının kullanma esaslarının belirtilmesini, kullanılmasına yönelik kuralların, yetki ve sorumlulukların belirlenmesini amaçlamaktadır.

**Esaslar:**

1. Bu taahhütname Hakkari Üniversitesi ve ..... firması tarafından imzalanır.
2. ..... firması bu taahhütname hükümleri, yükümlülüklerin hepsini kabul eder.
3. Taahhütname, işbu belgenin imzalanması ile yürürlüğe girer.
4. Taahhütname 2 (iki) kopya olarak hazırlanır. Bir kopyası ..... firmasında, diğer kopya ise Hakkari Üniversite'nde kalır.

**Yükümlülükler:**

1. Bu taahhütname, tedarikçi, taşeron, yüklenici ve müşteri ile imzalanan sözleşmelerde, sözleşmenin bir eki veya sözleşmenin içerisinde ayrı bir bölüm olarak yer alabileceği gibi, bir sözleşmeye bağlı olmadan da karşılıklı imzalanarak yürürlüğe alınır.
2. Hakkari Üniversitesi tarafından, ..... firmasına aktarılan yada hizmet esnasında ..... firması tarafından elde edilen kişisel verilerde, ..... firması 6698 sayılı Kişisel Verilerin Korunması Kanununda ve kanuna ilişkin diğer yasa, yönetmelik ve tebliğlerde yer alan sorumluluklarını yerine getirdiğini ve getireceğini ve işin ifası gereği kendisine aktarılan kişisel verilerin korunmasına yönelik gerekli idari ve teknik tedbirleri aldığını ve alacağını, kendi personellerini yeterli düzeyde eğittiğini ve eğiteceğini taahhüt eder.
3. Hakkari Üniversitesi tarafından, ..... fimasına aktarılan yada hizmet esnasında ..... firması tarafından elde edilen kurumsal verilerde, ..... firması Türkiye Cumhuriyeti'nin konu ile ilgili

tüm yasa, yönetmelik, genelge, tebliğ ve mevzuatlarında yer alan sorumluluklarını yerine getirdiğini ve getireceğini ve işin ifası gereği kendisine aktarılan kurumsal verilerin korunmasına yönelik gerekli idari ve teknik tedbirleri aldığını ve alacağını, kendi personellerini yeterli düzeyde eğittiğini ve eğiteceğini taahhüt eder.

4. Hakkari Üniversitesi ve ..... firmasının bir birlerine aktaracakları kişisel, kurumsal her tür veri, ..../..../2023 tarihli sözleşmede belirtilen kapsam ve amaçlar dışında ve/veya açık rızaya dayanak olan aydınlatma metninde belirtilen amaçlar dışında işlenmeyecek, arşivlenmeyecek ve yurt içi veya yurt dışındaki üçüncü kişi veya kuruluşlara aktarılmayacaktır. Bu yönde bir ihtiyaç olması durumunda akdedilen sözleşmede, açık rızaya dayanak olan aydınlatma metinlerinde karşılıklı mutabakat ile değişiklik yapılabilecektir.
5. ISO 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Standardı ve Kişisel Verilerin Korunması Kanunu Hakkında Danışmanlık Hizmeti iş ile elde edilen ve/veya Hakkari Üniversitesi tarafından ..... firmasına aktarılan kişisel, kurumsal verilerde, verileri aktarılan kişilerin veya Hakkari Üniversitesi'nin aydınlatılması, açık rıza alınması, veri işlemeye ve aktarılmaya ilişkin gerekli idari ve teknik tedbirlerin alınması ..... firması sorumluluğunda olup, bu aşamalardaki tüm yükümlülükler ..... firması tarafından yerine getirilecektir. Oluşacak maddi ve manevi zarardan ..... firması sorumlu olacaktır.
6. Kanunlarda veri saklamaya ilişkin yükümlülüklerin öngörülmüş hali saklı kalmak koşuluyla; kişisel, kurumsal verilerin işlenme sebebinin ortadan kalkması ile birlikte ..... firmasına aktarılmış olan veya ..... firmasının Hakkari Üniversitesi adına elde ettiği kişisel, kurumsal verilerin kayıtlı bulunduğu her türlü medya ve ortamı imza karşılığında Hakkari Üniversitesi'ne teslim edilir. Bununla birlikte, Hakkari Üniversitesi'ne iade edilemeyip firma nezdinde kalan kayıtları silme ve yok etme yükümlülüğü ..... firmasına aittir.
7. İlgili yasal kurumlar, denetim otoriteleri ve veri sahipleri tarafından Hakkari Üniversitesi'nden talep edilen bilgi ve belgelerin teslimi, ..... firmasına iletilmesinden itibaren firmaca 3 gün içerisinde yerine getirilmesi gerekmektedir.
8. ..... firmasının iş bu Taahhütname'ye, imzalanan sözleşmeye veya yürürlükteki mevzuata aykırı davranması dolayısıyla Hakkari Üniversitesi'nin

uğrayacağı zararlar, karşılaşacağı hukuki, idari ve cezai yaptırımlar ile ödemek zorunda kalabileceği tazminatlar için Hakkari Üniversitesi'nin ..... firmasına rücu hakkı saklıdır. ..... firması kendi kusur, kabahat ve ihmali sebebiyle, Hakkari Üniversitesi'nin uğrayacağı zararı karşılayacağını kabul, beyan ve taahhüt eder.

9. Taahhütname, Türk hukukuna tabi olacaktır. Taahhütname'den kaynaklanan ihtilaflarda Hakkari Mahkemeleri yetkilidir.

Bahar ÖĞÜR
Tekniker