KATEGORİ 1 · UYUM VE SÜRDÜRÜLEBİLİRLİK DANIŞMANLIKLARI

Kişisel Veri Yönetim Sistemi (KVYS/PIMS) Uyum Danışmanlığı ve İç Tetkik

ISO/IEC 27701

KVKK ve GDPR yükümlülüklerini, uluslararası denetlenebilir ve sertifikalandırılabilir bir mahremiyet yönetim sistemine (PIMS) dönüştüren bağımsız standart uyum danışmanlığı.

ISO 27701 danışmanlığı · PIMS · KVYS · GDPR uyum · DPIA · veri sorumlusu veri işleyen

KATEGORİ
Uyum ve Sürdürülebilirlik Danışmanlıkları

TİPİK SÜRE
Tipik program 4–7 ay · ISO 27001 mevcutsa 3–4 aya kadar kısalır

KİMLER İÇİN
Yurt dışına veri aktaran veya AB'de yerleşik ilgili kişilerin verisini işleyen kuruluşlar; veri işleyen sıfatıyla hizmet veren teknoloji ve BPO şirketleri; büyük ölçekli özel nitelikli veri işleyen sağlık ve sigorta kuruluşları.

1 Hizmetin Tanımı

Bu hizmet, kurumunuzun işlediği kişisel verilerin (PII) güvenliğini ve mahremiyetini sağlamak amacıyla KVKK, GDPR ve diğer uluslararası veri koruma regülasyonlarını kapsayan stratejik bir danışmanlık modelidir. Güncellenen yapısıyla kendi başına bağımsız ve tam kapsamlı bir yönetim standardı olan ISO 27701; "Veri Sorumlusu (Controller)" ve "Veri İşleyen (Processor)" rollerinize uygun olarak kişisel veri yönetim süreçlerinizi uluslararası denetlenebilir, sertifikalandırılabilir ve kanıtlanabilir bir yönetim sistemine dönüştürür.

2 Neden Gereklidir?

Günümüzde KVKK veya GDPR gibi yasal mevzuatlara uyum, sadece avukatlar tarafından hazırlanan aydınlatma metinleri veya sözleşmelerle sağlanamaz. Kurumların, kişisel verilerin toplanmasından imhasına kadar geçen tüm süreçte teknik ve idari güvenlik tedbirlerini nasıl uyguladığını uluslararası standartlarda ispat etmesi beklenmektedir. Veri ihlallerinin milyonlarca liralık idari para cezalarına ve geri dönülemez itibar kayıplarına yol açtığı bu dönemde ISO 27701, hukuk ile bilgi teknolojileri arasındaki boşluğu kapatır.

YAPTIRIM VE RİSK EŞİĞİ
KVKK tarafında veri güvenliği yükümlülüklerinin ihlali 2026 yılı için 256.357 ₺ – 17.092.242 ₺; GDPR tarafında ise küresel yıllık cironun %4'üne kadar idari para cezasına konu olabilmektedir.

3 Yasal ve Normatif Dayanak

- ISO/IEC 27701
- 6698 sayılı KVKK
- AB Genel Veri Koruma Tüzüğü (GDPR)
- Yurt dışına veri aktarımına ilişkin düzenlemeler

4 Sağladığı Katma Değer

Küresel güven ve GDPR uyumu

Uluslararası müşterilerinize, iş ortaklarınıza ve regülatörlere kişisel verileri sadece yerel yasalara göre değil, global ISO standartlarına göre koruduğunuzu resmî bir sertifika ile kanıtlamanızı sağlar.

Bağımsız ve kapsamlı yönetişim

ISO 27701, bir eklenti olmanın ötesine geçerek mahremiyet ve veri koruma süreçlerini kendi başına, uçtan uca yönetebilen bağımsız bir standart olarak kurgulanmıştır.

Hukuk ve BT entegrasyonu

Kanunların soyut hukuki gereksinimlerini, IT ve bilgi güvenliği ekiplerinin uygulayabileceği somut ve ölçülebilir teknik kontrollere dönüştürür.

Denetime tam hazırlık — sıfır uygunsuzluk hedefi

ISO 27701 yetkinliğine sahip uzmanlarımızca yapılan bağımsız iç tetkik simülasyonları ile dış belgelendirme riski ortadan kaldırılır.

5 Hizmet Kapsamı ve Metodoloji

AŞAMA 1

Mevcut Durum Analizi ve Kapsam Belirleme

Kurumun Veri Sorumlusu ve/veya Veri İşleyen şapkalarının analiz edilmesi. Mevcut KVKK/GDPR süreçleri ile ISO 27701 standardının bağımsız gereklilikleri arasındaki boşlukların tespit edilmesi.

AŞAMA 2

PII Risk Değerlendirmesi

Kişisel Veri Envanteri üzerinden Mahremiyet Etki Değerlendirmesi (PIA/DPIA) yapılarak risklerin analiz edilmesi ve risk işleme planlarının oluşturulması.

AŞAMA 3

Dokümantasyon ve Yönetişim Tasarımı

Mahremiyet politikaları, veri ihlali iletişim prosedürleri, veri sahibi başvuru süreçleri, aydınlatma metinleri ve formlar dâhil olmak üzere kurum kültürüne uygun tüm doküman setinin uçtan uca / sıfırdan hazırlanması.

AŞAMA 4

Eğitim ve İşletim

Veri mahremiyeti ve güvenliği farkındalık eğitimleri; veri saklama, maskeleme, anonimleştirme ve imha süreçlerinin sahada hayata geçirilmesi.

AŞAMA 5

İç Tetkik ve YGG

KVYS performansının bağımsız denetçilerimizce ölçülmesi, bulguların DÖF ile kapatılması ve sertifikasyon süreçlerinde teknik refakat.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ ISO 27701 Mevcut Durum (Gap) Analizi Raporu ve Proje Yol Haritası
- ✓ Kapsamlı Kişisel Veri (PII) Envanteri ve Mahremiyet Risk Değerlendirme Matrisi
- ✓ KVYS Uygulanabilirlik Bildirgesi (SoA)
- ✓ Kuruma özel KVYS dokümantasyon seti (politika, prosedür, iş süreçleri)
- ✓ Personel veri mahremiyeti farkındalık eğitim kayıtları
- ✓ Bağımsız iç tetkik raporu, DÖF kayıtları ve YGG yönetici özeti sunumu

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Akredite belgelendirme kuruluşlarının ISO 27701 Aşama 1 ve Aşama 2 denetimlerinden sorunsuz geçilerek kişisel veri koruma standartları belgelendirilir.
- ✓ KVKK ve GDPR uyumu, yasal bir zorunluluk olmaktan çıkıp kurumsal bir refleks ve uluslararası bir güven unsuruna dönüşür.
- ✓ Veri ihlali, sızıntı veya çalışan hatasından kaynaklanabilecek idari para cezası ve itibar kaybı riskini minimize eden sürdürülebilir bir mahremiyet yönetimi altyapısı kurulur.

7 Sık Sorulan Sorular

ISO 27001 olmadan ISO 27701 alınabilir mi?

Standardın güncel yapısı ISO 27701'i bağımsız olarak sertifikalandırılabilir hâle getirmiştir. Buna karşın mevcut bir BGYS, süreyi ve maliyeti belirgin biçimde düşürür.

ISO 27701 belgesi KVKK uyumu anlamına gelir mi?

Belge tek başına yasal uyumun yerine geçmez; ancak KVKK m. 12 kapsamındaki teknik ve idari tedbirlerin varlığını ve işletildiğini uluslararası düzeyde kanıtlayan en güçlü araçtır.

Yurt dışı müşterilerimiz denetim talep ediyor, bu belge yeterli olur mu?

Çoğu durumda evet. ISO 27701 sertifikası, müşteri denetimlerinde tekrar tekrar yürütülen soru seti süreçlerini kısaltan yaygın kabul görmüş bir güvence aracıdır.

8 Etiketler

ISO 27701 danışmanlığı · PIMS · KVYS · GDPR uyum · DPIA · veri sorumlusu veri işleyen · kişisel veri envanteri · mahremiyet etki değerlendirmesi

Bu hizmet, tam hizmet kataloğunun bir parçasıdır. Diğer 11 hizmet ve bütüncül paketler hakkında bilgi için Genel Broşür'e başvurabilirsiniz. Bu doküman bilgilendirme amaçlıdır; hukuki mütalaa veya taahhüt niteliği taşımaz.