



# ISO/IEC 27701:2025 GEÇİŞ SÜRECİ HAKKINDA DUYURU

## ANNOUNCEMENT ON THE ISO/IEC 27701:2025 TRANSITION PROCESS

| Doküman No. / Document No. | Yürürlük / Effective Date |
|----------------------------|---------------------------|
| WD-27701-01 • Rev.01       | 26.07.2026                |

**TR** ISO/IEC 27701 standardının 2025 sürümü yayımlanmış ve Kişisel Veri Yönetim Sistemi belgelendirmesine ilişkin geçiş süreci başlatılmıştır. Yeni sürümle birlikte ISO/IEC 27701, ISO/IEC 27001 ve ISO/IEC 27002'ye bağlı bir ek standart olma yapısından çıkarılarak bağımsız bir yönetim sistemi standardı hâline getirilmiştir.

**EN** The 2025 edition of ISO/IEC 27701 has been published and the transition process for Privacy Information Management System certification has commenced. Under the new edition, ISO/IEC 27701 has been transformed from an extension dependent on ISO/IEC 27001 and ISO/IEC 27002 into a stand-alone management system standard.

### 1. Yeni sürümde öne çıkan değişiklikler

#### Key changes introduced by the new edition

- Madde 4-10'un ISO yönetim sistemi standartlarının uyumlaştırılmış yapısına göre yeniden düzenlenmesi.  
*Clauses 4-10 have been aligned with the harmonized structure of ISO management system standards.*
- Bağımsız Kişisel Veri Yönetim Sistemi belgelendirmesine imkân sağlanması.  
*Stand-alone Privacy Information Management System certification is now possible.*
- Gizlilik risk değerlendirmesi, risk işleme ve artık risk kabulü şartlarının güçlendirilmesi.  
*Privacy risk assessment, risk treatment and residual-risk acceptance requirements have been strengthened.*
- PII güvenliğini destekleyen bilgi güvenliği programı gerekliliklerinin açıklığa kavuşturulması.  
*Requirements for the information security programme supporting PII security have been clarified.*
- Veri sorumlusu ve veri işleyen kontrollerinin yeniden numaralandırılması ve Ek A altında yeniden yapılandırılması.  
*Controls for PII controllers and processors have been renumbered and restructured under Annex A.*
- Ek B'nin normatif uygulama kılavuzu hâline getirilmesi.  
*Annex B has become normative implementation guidance.*
- Yapay zekâ destekli veri işleme ve sınır ötesi veri aktarımı gibi güncel gizlilik risklerinin daha açık ele alınması.  
*Emerging privacy risks, including AI-driven data processing and cross-border transfers, are addressed more explicitly.*

### 2. Geçiş takvimi

#### Transition timeline

**TR** Mevcut ISO/IEC 27701:2019 sertifikasına sahip kuruluşların ISO/IEC 27701:2025 sürümüne geçişlerini 31 Ekim 2027 tarihine kadar tamamlamaları gerekmektedir.

**EN** Organizations currently certified to ISO/IEC 27701:2019 are required to complete their transition to ISO/IEC 27701:2025 by 31 October 2027.

**TR** Geçiş denetimi; yeniden belgelendirme denetimiyle birlikte, gözetim denetimiyle birlikte veya ayrı bir geçiş denetimi olarak gerçekleştirilebilir.

**EN** The transition audit may be conducted together with a recertification audit, together with a surveillance audit or as a separate transition audit.

| Denetim yöntemi / Audit method                   | Türkçe uygulama                           | English application                                     |
|--------------------------------------------------|-------------------------------------------|---------------------------------------------------------|
| Yeniden belgelendirme ile / With recertification | En az 0,5 denetçi-gün ilave geçiş süresi. | At least 0.5 auditor-day of additional transition time. |
| Gözetim ile / With surveillance                  | En az 1,0 denetçi-gün ilave geçiş süresi. | At least 1.0 auditor-day of additional transition time. |
| Ayrı geçiş denetimi / Separate transition audit  | En az 1,0 denetçi-gün geçiş süresi.       | At least 1.0 auditor-day of transition time.            |

**TR** Belirtilen süreler asgari sürelerdir. Kuruluşun büyüklüğü, kapsamı, PII işleme faaliyetlerinin karmaşıklığı, lokasyon sayısı, teknolojik altyapısı ve veri sorumlusu/veri işleyen rolleri dikkate alınarak ilave süre belirlenebilir.

**EN** These are minimum durations. Additional time may be determined based on the organization's size, scope, complexity of PII-processing activities, number of locations, technological infrastructure and controller/processor roles.



### 3. Sertifikalı kuruluşların yapması gerekenler

#### Actions required from certified organizations

- ISO/IEC 27701:2019 ve ISO/IEC 27701:2025 arasında kuruluşa özgü boşluk analizi gerçekleştirilmesi.  
*Perform an organization-specific gap analysis between ISO/IEC 27701:2019 and ISO/IEC 27701:2025.*
- PIMS kapsamı, PII işleme faaliyetleri ve veri sorumlusu/veri işleyen rollerinin gözden geçirilmesi.  
*Review the PIMS scope, PII-processing activities and controller/processor roles.*
- Gizlilik risk değerlendirmesi ve risk işleme süreçlerinin güncellenmesi.  
*Update privacy risk assessment and risk treatment processes.*
- Bilgi güvenliği programının ve ilgili güvenlik kontrollerinin dokümanite edilmesi.  
*Document the information security programme and relevant security controls.*
- Uygulanabilirlik Beyanının ISO/IEC 27701:2025 Ek A yapısına göre revize edilmesi.  
*Revise the Statement of Applicability according to the ISO/IEC 27701:2025 Annex A structure.*
- Politika, prosedür, form ve kayıtların yeni madde ve kontrol numaralarına göre güncellenmesi.  
*Update policies, procedures, forms and records to the new clause and control identifiers.*
- İlgili personele eğitim ve farkındalık sağlanması.  
*Provide training and awareness to relevant personnel.*
- ISO/IEC 27701:2025'i kapsayan iç denetim ve yönetimin gözden geçirmesinin tamamlanması.  
*Complete an internal audit and management review covering ISO/IEC 27701:2025.*

### 4. Geçiş denetimi ve belgelendirme kararı

#### Transition audit and certification decision

**TR** Geçiş denetimi yalnızca doküman incelemesine dayanmayacaktır. Özellikle teknolojik bilgi güvenliği kontrollerinin, risk işleme faaliyetlerinin ve güncellenen süreçlerin uygulama kanıtları örneklenerek değerlendirilecektir.

**EN** The transition audit will not rely solely on document review. Implementation evidence will be sampled, particularly for technological information security controls, risk treatment activities and updated processes.

**TR** Geçiş denetiminin tamamlanması, varsa uygunsuzlukların kapatılması, teknik inceleme ve olumlu belgelendirme kararının ardından ISO/IEC 27701:2025 referanslı güncel sertifika düzenlenecektir.

**EN** Following completion of the transition audit, closure of any nonconformities, technical review and a positive certification decision, an updated certificate referencing ISO/IEC 27701:2025 will be issued.

### 5. Geçişin zamanında tamamlanmamasının sonuçları

#### Consequences of not completing transition on time

**TR** ISO/IEC 27701:2025 geçişini 31 Ekim 2027 tarihine kadar tamamlamayan kuruluşların ISO/IEC 27701:2019 sertifikaları geçiş dönemi sonrasında sürdürülemez.

**EN** ISO/IEC 27701:2019 certificates of organizations that do not complete transition to ISO/IEC 27701:2025 by 31 October 2027 cannot be maintained beyond the transition period.

### 6. İletişim

#### Contact

**TR** Geçiş planlaması, denetim yöntemi, denetim süresi ve hazırlanması gereken kanıtlar hakkında bilgi almak için Sigmacert Belgelendirme ve Operasyon Birimi ile iletişime geçebilirsiniz.

**EN** For information regarding transition planning, audit method, audit duration and required evidence, please contact the Sigmacert Certification and Operations Department.

|                                        |                                                                             |
|----------------------------------------|-----------------------------------------------------------------------------|
| <b>Kuruluş / Organization</b>          | SIGMACERT                                                                   |
| <b>İlgili Birim / Contact Function</b> | Belgelendirme ve Operasyon Birimi / Certification and Operations Department |
| <b>Konu / Subject</b>                  | ISO/IEC 27701:2025 Geçiş / ISO/IEC 27701:2025 Transition                    |