PRIVACY PROFESSIONALS
شركة محترفو الخصوصية لحلول الأعمال

# من حماية البيانات إلى تعزيز الثقة

## دليل شامل لفهم شهادة ISO 27701 ومتطلباتها

## مقدمة: ما هو المعيار ISO 27701 ولماذا هو مهم؟

تم إصدار معيار ISO 27701 في أغسطس 2019 كامتداد لمعيار ISO 27001 ودليل الممارسات ISO 27002، بهدف وضع إطار عملي لإدارة خصوصية المعلومات (PIMS). يحدد المعيار متطلبات وإرشادات تساعد المؤسسات على إدارة ومعالجة وحماية بيانات التعريف الشخصية (PII) بما يتوافق مع القوانين المحلية والدولية مثل GDPR.

تكمن أهمية المعيار في كونه لا يقتصر على نوع محدد من المؤسسات، بل يمكن تطبيقه على مختلف القطاعات بغض النظر عن حجمها أو موقعها، مما يجعله أداة أساسية لتعزيز الشفافية والامتثال وبناء الثقة مع العملاء والجهات التنظيمية.

## شهادة ISO 27701 وانتشارها الدولي

شهدت شهادة ISO 27701 انتشارًا متزايدًا عالميًا باعتبارها معيارًا دوليًا معترفًا به حماية البيانات ومكملًا لـ ISO 27001 ويزداد تبنيها بشكل خاص في القطاعات التي تتطلب حماية صارمة للبيانات الشخصية مثل مثل قطاع التقنية والصحة والخدمات المالية، وكذلك في الأسواق التي تفرض لوائح خصوصية قوية مثل GDPR و CCPA .

## القطاعات الأكثر تبنيًا للمعيار

يُعَدّ معيار ISO 27701 من أكثر الأطر المرجعية انتشارًا في القطاعات ذات الحساسية العالية تجاه البيانات الشخصية، حيث يُمكّن المؤسسات من مواءمة أنظمة إدارة أمن المعلومات مع متطلبات الخصوصية المتزايدة التعقيد. وتشير الممارسات الدولية إلى أن أبرز القطاعات التي أظهرت مستويات مرتفعة من التبني هي:

### القطاع الصحي

يعد هذا القطاع من أكثر القطاعات تعرضًا للمخاطر نظرًا لاعتماده على معالجة بيانات صحية شديدة الحساسية، مما يجعل الحصول على الشهادة خطوة استراتيجية لضمان الامتثال لمتطلبات حماية البيانات وحوكمة المعلومات الطبية.

### الخدمات المالية والمصرفية

تتعامل المؤسسات المالية مع بيانات مالية وشخصية بالغة الأهمية، ويُعتبر تطبيق ISO 27701 وسيلة لتقليل مخاطر الامتثال وتعزيز ثقة العملاء والمستثمرين.

### القطاع الحكومي والقطاع العام

مع توسع مبادرات التحول الرقمي، أصبح تطبيق المعيار ضرورة لتمكين الحكومات من حماية بيانات المواطنين وضمان التوافق مع القوانين المحلية والدولية ذات الصلة.

### قطاع الاتصالات وتقنية المعلومات

يشهد هذا القطاع إقبالا متزايدًا على الشهادة، خصوصًا لدى مزوّدي الخدمات السحابية وشركات البرمجيات التي تدير كميات ضخمة من بيانات المستخدمين على المستوى العالمي.

### القطاع التعليمي

دفع تزايد الاعتماد على الأنظمة الإلكترونية في إدارة بيانات الطلاب والمعلمين المؤسسات التعليمية إلى تبني المعيار لضمان حماية البيانات والامتثال للتشريعات.

**إن هذا الانتشار يعكس إدراكًا متناميًا لأهمية الشهادة بوصفها وسيلة استراتيجية لتعزيز الثقة المؤسسية وتدعيم قدرات الامتثال ضمن بيئة تنظيمية تتسم بالتطور المستمر.**

## أمثلة لقطاعات حصلت على شهادة ISO 27701 في دول الخليج

تُظهر التجارب الإقليمية في دول الخليج أن معيار ISO 27701 لم يعد يُنظر إليه كخيار تكميلي، بل كأداة محورية لترسيخ ممارسات حوكمة الخصوصية. فقد اتجهت عدة قطاعات إلى اعتماده، ومن أبرزها:

### القطاع المالي

بادرت بعض البنوك في المنطقة إلى الحصول على الشهادة بهدف تعزيز نظم إدارة البيانات، والاستجابة لمتطلبات الجهات التنظيمية المحلية والدولية.

### القطاع الصحي

اعتمدت مؤسسات رعاية صحية ومزوّدو حلول تقنية طبية المعيار لضمان الامتثال وحماية بيانات المرضى، مما يعكس إدراكًا متزايدًا لمخاطر انتهاك الخصوصية في هذا المجال.

### القطاع الحكومي وقطاع الاتصالات وتقنية المعلومات

أظهرت بعض الهيئات الحكومية وشركات الاتصالات والتقنية توجهًا استراتيجيًا نحو دمج ISO 27701 في أنظمتها، وذلك لضمان حماية بيانات الأفراد ومواكبة مسار التحول الرقمي.

إن تبني هذه القطاعات للشهادة يُعَدّ مؤشرًا على التحول نحو حوكمة وقائية تستند إلى المعايير الدولية، بما يعزز قدرة المؤسسات الخليجية على المنافسة عالميًا وضمان الامتثال للمتطلبات التنظيمية الصارمة.

## التكامل بين ISO 27701 ونظام حماية البيانات الشخصية (PDPL) في المملكة العربية السعودية

يُعَدّ نظام حماية البيانات الشخصية (PDPL) الإطار التشريعي الملزم على المستوى الوطني، إذ يهدف إلى تنظيم آليات جمع البيانات الشخصية ومعالجتها وتخزينها بما يضمن صون حقوق الأفراد وتعزيز مبادئ الشفافية والمساءلة. وفي المقابل، يمثل ISO 27701 إطارًا دوليًا مرنًا يوفّر منهجية عملية لإنشاء نظام إدارة معلومات الخصوصية (PIMS) داخل منظومة إدارة أمن المعلومات (ISMS) المبنية على ISO 27001.

إن الجمع بين المتطلبات الإلزامية المحلية (PDPL) والممارسات المرجعية العالمية (ISO 27701) يتيح للمنظمات بناء نظام متكامل يعزز الامتثال القانوني ويرسخ حوكمة الخصوصية. ويتجسد هذا التكامل في أربعة محاور رئيسية:

### توحيد السياسات والإجراءات التنظيمية

عبر مواءمة الأسس النظامية لمعالجة البيانات مع الضوابط التي يحددها PDPL.

### تعزيز حقوق أصحاب البيانات

من خلال توفير آليات عملية لتطبيق الحقوق الجوهرية مثل الوصول، التصحيح، الحذف، ونقل البيانات.

### إدارة حوادث الخصوصية بكفاءة

وذلك بفضل ما يقدمه المعيار من أدوات لرصد الحوادث والإبلاغ عنها ضمن الأطر الزمنية التي يفرضها النظام المحلي.

### حماية البيانات الحساسة

عبر اعتماد ضوابط أمنية وتقنية متقدمة تتماشى مع متطلبات البيئة التنظيمية الوطنية.

وبهذا يصبح ISO 27701 ليس مجرد أداة مساندة، بل إطارًا استراتيجيًا يمكّن المنظمات من الجمع بين الامتثال المحلي والتوافق الدولي على نحو يعزز مكانتها التنافسية.

## ما الذي تكسبه المنظمات من ISO 27701؟

اعتماد ISO 27701 لا يُنظر إليه كخطوة امتثال إجرائية فحسب، بل كاستثمار استراتيجي طويل الأمد ينعكس على ثقة السوق واستدامة الأعمال. ومن أبرز الفوائد العملية التي يمكن رصدها:

### 1- تعزيز الثقة المؤسسية:

إذ يشكّل الحصول على الشهادة دليلًا موثقًا على التزام المنظمة بحماية البيانات، الأمر الذي يرسّخ ثقة العملاء والشركاء والجهات التنظيمية.

### 2-تسريع الامتثال

من خلال توفير إطار جاهز يمكّن المنظمات من اختصار الزمن والجهد في مواءمة سياساتها مع التشريعات المعقدة مثل GDPR وPDPL.

### 3- الجاهزية للتدقيق والرقابة

يقدّم المعيار منهجية واضحة لإعداد أدلة الامتثال، مما يسهل اجتياز عمليات التدقيق الداخلي والخارجي بكفاءة عالية.

### 4. المواءمة عبر الحدود

عبر ربط الالتزامات الوطنية بمقتضيات اللوائح الدولية مثل GDPR، بما يتيح للمنظمات إدارة عملياتها محليًا ودوليًا بانسجام تشريعي متكامل.

وعليه، يمكن القول إن تطبيق ISO 27701 يمثل نقطة التقاء بين الإطار التنظيمي المحلي والمعايير الدولية ، مما يحوّله إلى عنصر محوري في استراتيجيات الحوكمة والامتثال.

## تكامل ISO 27701 مع المعايير الأخرى

لا يعمل ISO 27701 بمعزل عن غيره من الأطر المعيارية، بل يتكامل بصورة وثيقة مع منظومة معايير أمن المعلومات والخصوصية الدولية. وكما ذكرنا سابقًا، يُعَدّ امتدادًا طبيعيًا لمعيار ISO 27001، حيث يضيف طبقة متخصصة لإدارة وحماية البيانات الشخصية ضمن نظام إدارة أمن المعلومات. (ISMS)

**ومن أبرز نقاط التكامل:**

### ISO 27001

يُعَدّ المعيار الأساسي الذي يضع البنية التحتية لنظام إدارة أمن المعلومات. ولا يمكن الحصول على ISO 27701 دون وجود ISMS قائم على ISO 27001، مما يعكس العلاقة التكاملية بينهما.

### ISO 27002

يقدّم إرشادات مفصلة لضوابط أمن المعلومات، ويُوسّع ISO 27701 هذه الضوابط لتشمل متطلبات الخصوصية بشكل مباشر.

### ISO 29100

يضع إطارًا مفاهيميًا عالميًا للخصوصية، بينما يترجم ISO 27701 هذا الإطار إلى متطلبات عملية قابلة للتنفيذ.

### ISO 27005

يركّز على إدارة مخاطر أمن المعلومات، ويُعزّز ISO 27701 هذا الجانب بإضافة اعتبارات متعلقة بمخاطر الخصوصية.

### ISO 27018

يختص بحماية البيانات الشخصية في بيئات الحوسبة السحابية، ويتكامل مع ISO 27701 لتوفير مستوى أعلى من الضمانات التقنية والتنظيمية.

إن هذا الترابط يُمكّن المنظمات من بناء نظام متكامل لإدارة الأمن والخصوصية، حيث تُعالج قضايا أمن المعلومات والامتثال التشريعي من خلال إطار موحد يقلل التكلفة التشغيلية ويُعزز الكفاءة.

## أبرز الفروقات بين شهادتي ISO 27001 و ISO 27701

### 1. الهدف والنطاق:

- يركّز ISO 27001 على حماية جميع أشكال المعلومات داخل المنظمة، سواء كانت مالية أو تشغيلية أو موارد بشرية أو بيانات عملاء، وذلك عبر ضمان السرية والتكامل والتوافر.

- بينما يضيف ISO 27701 بُعدًا متخصصًا يتعلق بالبيانات الشخصية (PII)، مع التركيز على حماية الخصوصية والامتثال للتشريعات العالمية مثل GDPR وCCPA و HIPAA.

### 2. طبيعة المتطلبات:

- يتضمن ISO 27001 بنودًا رئيسية (من 4 إلى 10) تضع الأسس العامة لنظام إدارة أمن المعلومات، مدعومة بملحق "أ" الذي يضم 114 ضابطًا أمنيًا يمكن تطبيقها وفقًا لتقييم المخاطر.

- أما ISO 27701 فيضيف بنودًا جديدة (من 5 إلى 8) مكرّسة لحماية البيانات الشخصية، وتشمل إرشادات عملية لممارسات الخصوصية وضوابط إضافية لكل من متحكم البيانات ومعالج البيانات.

### 3. إمكانية الاعتماد:

- يمكن الحصول على شهادة ISO 27001 بشكل مستقل، فهي تمثل المعيار المرجعي الأساسي لإنشاء نظام إدارة أمن المعلومات.

- في المقابل، لا يُمنح ISO 27701 إلا كامتداد لـ ISO 27001، أي أنه لا يُعتمد بمعزل عنه، وإنما يُضاف فوقه لتعزيز بعد الخصوصية.

### 4. العلاقة باللوائح الدولية:

- يُعتبر ISO 27001 إطارًا عامًا يوفّر أساسًا للامتثال لمعايير أمن المعلومات دون التركيز على تشريع محدد.

- بينما صُمم ISO 27701 بشكل مباشر لتمكين المنظمات من إثبات توافقها مع قوانين الخصوصية الأكثر تعقيدًا، وعلى رأسها اللائحة الأوروبية لحماية البيانات GDPR، مع إمكانية مواءمته مع تشريعات أخرى.

## هل يتطلب الحصول على شهادة ISO 27701 وجود شهادة ISO 27001 مسبقًا؟

نعم، يُشترط للحصول على شهادة ISO 27701 وجود نظام إدارة أمن معلومات قائم ومتوافق مع ISO 27001. ويعود السبب إلى أن ISO 27701 ليس معيارًا مستقلًا بل يمثل امتدادًا بنيويًا يُضاف فوق ISO 27001 ليغطي جانب الخصوصية.

إن ISO 27001 يضع الأساس لبناء إطار شامل لحماية المعلومات استنادًا إلى السرية والتكامل والتوافر، بينما يأتي ISO 27701 لتعزيز هذا الإطار من خلال إدخال ضوابط إضافية موجهة لحماية البيانات الشخصية (PII) والامتثال للتشريعات المرتبطة بها.

**وعمليًا، يمكن للمنظمات اتباع مسارين:**

### التطبيق المرحلي

الحصول أولًا على ISO 27001 ثم التوسع لاحقًا بإضافة ISO 27701.

### التطبيق المتوازي

تنفيذ المعياريين معًا ضمن إطار واحد والحصول على الشهادتين في الوقت ذاته.

وبالتالي، فإن ISO 27001 يُعَدّ شرطًا مسبقًا لا غنى عنه، ليس فقط من الناحية الشكلية للحصول على الاعتماد، وإنما أيضًا من الناحية العملية لضمان وجود بنية مؤسسية قادرة على استيعاب نظام إدارة خصوصية المعلومات (PIMS).

## ما الفوائد التي يوفرها ISO 27701 عند عدم وجود ISO 27001؟

من الناحية النظرية، قد تحاول بعض المنظمات الاستفادة من ISO 27701 بشكل منفصل، إلا أن ذلك يُنتج فوائد محدودة للغاية. فالمعيار صُمِّم ليُبنى على ISO 27001، وفي غياب الأخير يفقد جزءًا كبيرًا من قوته.

- في هذه الحالة، يقتصر دور ISO 27701 على توفير إرشادات لحماية البيانات الشخصية وضمان الامتثال الجزئي للتشريعات مثل GDPR.
- يمكن أن يُسهم في رفع مستوى الشفافية مع العملاء وأصحاب المصلحة، عبر توضيح كيفية التعامل مع البيانات الشخصية.
- يتيح تحديدًا أوضح للأدوار والمسؤوليات (المتحكم والمعالج) وتحسين إدارة عقود معالجة البيانات.

إلا أن غياب ISO 27001 يترك فجوة كبيرة، لأن المنظمات تفتقر إلى إدارة أمن معلومات شاملة تغطي جميع أنواع البيانات، وليس فقط البيانات الشخصية. وعليه، فإن القيمة الحقيقية لـ ISO 27701 تتحقق فقط عند دمجه مع ISO 27001 ضمن إطار متكامل.

## هل يساهم ISO 27701 في الامتثال للقوانين العالمية لحماية البيانات؟

نعم، يُسهم معيار ISO 27701 بشكل مباشر في تمكين المنظمات من مواءمة أنظمتها مع التشريعات العالمية الخاصة بحماية البيانات الشخصية، وعلى رأسها اللائحة الأوروبية لحماية البيانات GDPR. فهو يوفّر إطارًا عمليًا لإدارة خصوصية المعلومات (PIMS) ضمن منظومة أمن المعلومات (ISMS)، بما يضمن تطبيق سياسات وضوابط تتماشى مع متطلبات تلك التشريعات.

ومع ذلك، ينبغي التأكيد على أن ISO 27701 لا يُمثل امتثالًا قانونيًا بحد ذاته، بل يُعَدّ أداة داعمة تساعد المنظمات على إثبات التزامها وتسهيل الامتثال للتشريعات الدولية.

## هل تضمن شهادة ISO 27701 الامتثال الكامل للقوانين مثل GDPR؟

لا، لا تُعدّ شهادة ISO 27701 ضمانًا كافيًا للامتثال الكامل للتشريعات مثل GDPR أو غيرها من القوانين المماثلة. فالمعيار، وإن كان يوفر إطارًا منهجيًا لإدارة خصوصية المعلومات (PIMS) ويُسهم في مواءمة الممارسات الداخلية مع المتطلبات التنظيمية، إلا أنه لا يغطي جميع الأبعاد القانونية والتشريعية.

**ذلك لأن الامتثال الكامل للتشريعات يتطلب:**

- تفسيرًا قانونيًا دقيقًا للمواد التنظيمية.
- تنفيذ سياسات محلية وإجراءات تشغيلية مفصّلة.
- الاستجابة لمتطلبات قانونية متغيرة تتجاوز نطاق المعيار.

وعليه، تُعتبر شهادة ISO 27701 خطوة أساسية داعمة تُمكّن المنظمات من إثبات التزامها، لكنها لا تُعادل شهادة امتثال قانوني، ولا يمكن الاعتماد عليها منفردة لضمان التوافق الشامل مع اللوائح مثل GDPR

## ما هي الفجوات التي لا تغطيها شهادة ISO 27701 في تطبيق قوانين حماية البيانات؟

على الرغم من أن ISO 27701 يُعَدّ إطارًا رائدًا لإدارة خصوصية المعلومات، إلا أن هناك فجوات واضحة تحدّ من قدرته على تحقيق امتثال شامل لقوانين حماية البيانات.

**من أبرز هذه الفجوات:**

### 1. غياب الأساس المستقل لإدارة أمن المعلومات:

يعتمد ISO 27701 بالكامل على ISO 27001. وبالتالي، لا يمكن اعتباره كافيًا بمفرده لتغطية جميع المخاطر المتعلقة بأمن المعلومات، بل يحتاج إلى بنية تحتية أمنية متكاملة.

### 2. تحديات التوافق بين الأطر التشريعية المختلفة:

في حين أن المعيار يوفّر إطارًا عامًا، إلا أن مواءمته مع تشريعات متباينة مثل GDPR وCCPA وPDPL تتطلب تخصيصًا إضافيًا يتجاوز ما هو منصوص عليه.

### 3. عدم شمول التفاصيل القانونية الدقيقة:

الامتثال القانوني يتطلب تفسير النصوص التشريعية، وإدارة حقوق الأفراد وفق الإجراءات القانونية المحلية. هذه الأبعاد لا يغطيها المعيار بشكل كامل.

### 4. محدودية معالجة المخاطر المعقدة للخصوصية:

لا يوفّر المعيار أدوات متكاملة لإجراء تقييمات أثر حماية البيانات (DPIA) التفصيلية، مما يترك فجوة في إدارة المخاطر ذات البعد الاجتماعي والقانوني.

### 5. التكيف مع التغيرات التنظيمية:

اللوائح تتغير بوتيرة سريعة، بينما يظل المعيار ثابتًا حتى يتم تحديثه رسميًا. وهذا يفرض على المنظمات إنشاء آليات متابعة مستقلة لا يوفرها المعيار.

### 6. الجوانب التقنية التشغيلية الخاصة بالقطاعات:

يضع المعيار ضوابط عامة، لكنه لا يعالج تفاصيل تطبيقية مرتبطة بقطاعات محددة (مثل الرعاية الصحية أو البنوك)، ما يستلزم الاعتماد على أطر أو إرشادات إضافية.

## هل توجد معايير أو أدوات تكمل فجوات تطبيق ISO 27701 في قوانين حماية البيانات؟

نعم، هناك مجموعة من المعايير والأدوات التي تُعَدّ مكملة لـ ISO 27701 وتساعد على سد الفجوات التي لا يغطيها المعيار بمفرده. هذه المكملات تُسهم في تعزيز القدرة المؤسسية على تحقيق امتثال شامل وتشغيلي مع القوانين الوطنية والدولية. **ومن أبرزها:**

### ISO 27001

يمثل الأساس البنيوي الذي يُبنى عليه ISO 27701. فبدون وجود نظام إدارة أمن المعلومات (ISMS) قوي، يظل تطبيق ISO 27701 محدودًا وغير مكتمل.

### ISO 27002

يقدم ضوابط تفصيلية لأمن المعلومات تساعد على ترجمة التوجيهات العامة في ISO 27701 إلى إجراءات عملية قابلة للتنفيذ.

### تقييم أثر حماية البيانات (DPIA):

أداة تنظيمية متقدمة تتطلبها تشريعات مثل GDPR، وتساعد على تحليل المخاطر المرتبطة بمعالجة البيانات الشخصية وتأثيرها على الخصوصية.

### تحليل الفجوات وإدارة المخاطر (Gap Analysis & Risk Assessment):

أدوات منهجية لقياس الفارق بين الوضع الحالي ومتطلبات التشريعات والمعايير، مما يمكّن المنظمات من تطوير خطط معالجة دقيقة.

### الأطر التشريعية المحلية والدولية:

مثل PDPL على المستوى المحلي، وGDPR وHIPAA وCCPA على المستوى الدولي. دمج هذه المتطلبات يضمن تغطية الأبعاد القانونية التي لا يتناولها المعيار.

### السياسات والبرامج الداخلية المتخصصة:

مثل برامج التدريب والتوعية، إدارة الحوادث الأمنية، وإجراءات التعاقد مع مزوّدي الخدمات، بما يضمن دمج الخصوصية في الثقافة المؤسسية اليومية.

## هل يساهم ISO 27701 في تسهيل الامتثال للوائح العالمية لحماية البيانات؟

نعم، يُسهم معيار ISO 27701 في تبسيط مسار الامتثال للوائح العالمية الخاصة بحماية البيانات، من خلال تقديم إطار موحد يمكن للمنظمات استخدامه كأساس لبناء أنظمة الخصوصية الداخلية. وبدلًا من الاضطرار إلى تطوير إجراءات منفصلة لكل تشريع، يوفّر المعيار مجموعة من الضوابط والإرشادات التي يمكن تكييفها بما يتوافق مع مختلف الأطر القانونية.

**تتجلى أبرز مظاهر التسهيل في:**

### توحيد الممارسات:

اعتماد هيكل واحد يربط بين الضوابط الأمنية وضوابط الخصوصية، مما يقلل من ازدواجية الجهود.

### تقليل التكلفة والوقت:

اختصار المراحل الأولية لتأسيس نظام خصوصية متكامل، وتوفير نقطة انطلاق جاهزة للامتثال.

### تسهيل التدقيق والرقابة:

إتاحة أدلة موثقة تمكّن الجهات التنظيمية والمراجعين من تقييم الالتزام بوضوح وسرعة.

### قابلية التوسع:

تصميم المعيار ليكون مرنًا وقابلًا للتطبيق في منظمات بمختلف الأحجام والقطاعات.

## ما هو تأثير ISO 27701 على الثقة وبناء سمعة الشركات عالميًا؟

اعتماد شهادة ISO 277091 يُمثل عاملًا استراتيجيًا مؤثرًا في تعزيز الثقة المؤسسية وبناء السمعة على الصعيدين المحلي والدولي. فالمنظمات التي تمتلك هذه الشهادة تُنظر إليها على أنها كيانات ملتزمة بأعلى معايير حماية البيانات، وهو ما ينعكس إيجابًا على مكانتها التنافسية.

**يتجلى الأثر في عدة مستويات رئيسية:**

### الثقة مع العملاء وأصحاب المصلحة:

تعكس الشهادة التزام المنظمة بإدارة خصوصية البيانات بمسؤولية، مما يعزز ثقة الأفراد في التعامل معها ومشاركتهم لبياناتهم الشخصية.

### تحسين السمعة المؤسسية:

يُنظر إلى المنظمات الحاصلة على الشهادة على أنها تلتزم بالمعايير الدولية وتستبق المتطلبات التشريعية، مما يمنحها صورة ذهنية قوية بوصفها جهة موثوقة.

### ميزة تنافسية في الأسواق العالمية:

الحصول على ISO 27701 يفتح المجال أمام فرص تجارية واستثمارية جديدة، خصوصًا في الأسواق التي تجعل من حماية البيانات شرطًا أساسيًا للشراكات أو العقود.

### تعزيز الثقافة المؤسسية الداخلية:

الشهادة لا تنعكس فقط خارجيًا، بل تُسهم أيضًا في ترسيخ وعي الموظفين بمسؤولياتهم تجاه الخصوصية، مما يعزز التزامًا جماعيًا يحمي صورة المنظمة على المدى الطويل.

## أهم الطرق التي تساعد المؤسسات على تبسيط إجراءات الالتزام بـ ISO 27701

تطبيق متطلبات ISO 27701 قد يبدو معقدًا في البداية نظرًا لتشابك الجوانب التقنية والتنظيمية والقانونية المرتبطة به، إلا أن هناك مجموعة من الممارسات التي تساعد على تبسيط الإجراءات وتحقيق الامتثال بكفاءة أعلى:

### الاعتماد على نظام إداري موحد

دمج نظام إدارة خصوصية المعلومات (PIMS) مع نظام إدارة أمن المعلومات (ISMS) وفق ISO 27001، بما يقلل من التكرار ويضمن التكامل بين الضوابط الأمنية وضوابط الخصوصية.

### استخدام أطر التوصيف (Mapping Frameworks):

ربط متطلبات ISO 27701 باللوائح المحلية والدولية مثل GDPR وPDPL، مما يسهّل على المنظمات الامتثال لمعايير متعددة دون ازدواجية في الجهود.

### توظيف الأدوات التقنية

الاستعانة بأنظمة الحوكمة وإدارة الامتثال الرقمية التي توفّر عمليات آلية للمراقبة والتدقيق، مما يقلل العبء الإداري ويحسّن دقة التنفيذ.

### تدريب وتوعية الموظفين:

الاستثمار في رفع مستوى الوعي حول خصوصية البيانات وأمن المعلومات، بحيث يصبح الالتزام جزءًا من الثقافة المؤسسية اليومية.

### المراجعة الدورية والتحسين المستمر:

إجراء تدقيقات داخلية منتظمة وتقييمات دورية لضمان استمرارية الامتثال وتطوير الإجراءات بما يتماشى مع المستجدات التنظيمية.

### تحديد الأدوار والمسؤوليات بوضوح:

وضع تعريفات دقيقة لمهام مسؤولي الخصوصية ومتحكمي البيانات والمعالجين، لتسريع القرارات وتقليل الالتباس التنظيمي.

### الاستعانة بخبرات متخصصة:

إشراك مستشارين أو خبراء في الامتثال يساعد على تسريع عملية التطبيق وتجاوز التحديات العملية.

## الخاتمة

يمثل معيار ISO 27701 ركيزة أساسية لربط حماية البيانات بالامتثال للتشريعات المحلية والدولية، حيث يوفّر إطارًا عمليًا يعزز الشفافية ويحد من المخاطر. ويسهم اعتماده في ترسيخ الثقة مع العملاء والجهات التنظيمية، مما يمنح المنظمات مكانة تنافسية أقوى في الأسواق العالمية. ومع تكامله مع ISO 27001، يتحول المعيار إلى أداة استراتيجية تدعم استدامة الأعمال وتعزز قدرة المؤسسات على مواجهة تحديات الخصوصية المستقبلية.

## بسمه السبيعي

خبيرة في حماية البيانات وحوكمة الذكاء الاصطناعي، عملت في جهات تنظيمية وتشريعية وأسهمت في تطوير استراتيجيات وطنية ولوائح معتمدة. تميز مسارها الاستراتيجي بدور وطني فعّال في بناء السياسات وتعزيز المبادرات الوطنية لتنظيم البيانات والذكاء الاصطناعي وتقليل المخاطر التقنية.

## فاطمة القحطاني

متخصصة في الأمن السيبراني وحوكمة الذكاء الاصطناعي، بخبرة في مراجعة الضوابط التنظيمية وتطبيق السياسات المؤسسية. أسهمت في تطوير أطر حوكمة متكاملة وفق المنهجيات الوطنية والدولية بما يعزز حماية البيانات والامتثال.

## جمانة اللقماني

مسؤولة حماية بيانات تركز على الامتثال وإدارة المخاطر، بخبرة في مراجعة العقود والسياسات وتحليل البيانات. شاركت في تطوير استراتيجيات لتحسين جودة البيانات وتطبيق ممارسات تعزز الشفافية والالتزام التشريعي.

# Think privacy
# Build trust


0501591111

Business@ppros.com.sa

www.ppros.com.sa