



# الدورة التدريبية: أمن المعلومات القانوني والامتثال للتشريعات الرقمية

مايو ٢٠٢٦ - ٠٨ - ٠٤

فيينا

(للشخص الواحد) € ٥٧٠٠

Ref: #CYB8448\_271773





## مقدمة الدورة التدريبية / لمحة عامة:

إنّ الفشل في الامتثال الرقمية وقوانين حماية البيانات من أهم التحديات في ظل التطور المتسارع للتقنية، أصبحت التشريعات ثقة العملاء، أو قوانين الخصوصية المحلية يمكن أن (GDPR) للوائح مثل اللائحة العامة لحماية البيانات التي تواجه المؤسسات. أمن المعلومات، المستشارين والإضرار بسمعة الشركة. تقدم هذه الدورة التدريبية يؤدي إلى غرامات باهظة، وفقدان الأمن اللازمة لدمج الأمن السيبراني مع المتطلبات القانونية، ومسؤولي الامتثال، المعرفة والمهارات المتخصصة لمختصي الامتثال. سيكتسب المشاركون القانوني، أهم اللوائح الدولية والمحلية، وأفضل القانونية. سنتناول في هذه الدورة مفاهيم في تقييم المخاطر القانونية للبيانات، وبناء إطار القدرة على وضع سياسات أمنية تتوافق مع القوانين، الممارسات لتحقيق إلى أحدث الأمن القانوني للبيانات، مما يضمن عمل المؤسسة ضمن حوكمة قوي. تهدف الدورة إلى بناء كوادر متخصصة خبراء أكاديميين بارزين مثل البروفيسور المعايير وأفضل الممارسات الدولية، مع الاستفادة الإطار القانوني. يستند المحتوى BIG هذه الدورة المعروف بأعماله في قانون الخصوصية وأمن المعلومات. دانيال ج. سولوف (Daniel J. Solove)، من إسهامات الرقمي والالتزام القانوني. لتمكين المؤسسات من تحقيق التوازن بين الابتكار يقدم BEN Training Center



## لأ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مديرو الأمن السيبراني.
- مسؤولو الامتثال والمخاطر.
- المستشارون القانونيون ومحامو الشركات.
- مديرو تقنية المعلومات.
- مسؤولو حماية البيانات (DPOs).
- البيانات الحساسة. الموظفون الإداريون في الأقسام التي تتعامل مع

## القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات التأمين.
- الرعاية الصحية.
- شركات التكنولوجيا.
- الجهات الحكومية وما في حكمها.
- الشركات متعددة الجنسيات.

## الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- الإدارة القانونية.
- إدارة الامتثال والحوكمة.
- إدارة تقنية المعلومات.
- إدارة المخاطر.



## أهداف الدورة التدريبية:

أُتقن المهارات التالية: بنهاية هذه الدورة التدريبية، سيكون المتدرب قد

- القانونية، فهم العلاقة بين الأمن السيبراني والتشريعات
- لحماية البيانات، القدرة على تفسير اللوائح القانونية الرئيسية
- تطبيق ضوابط أمنية تتوافق مع متطلبات الامتثال.
- وضع سياسات وإجراءات لحماية البيانات الحساسة.
- المعلومات، إجراء تقييم للمخاطر القانونية المتعلقة بأمن
- التعامل مع حوادث انتهاك البيانات من منظور قانوني.
- بناء إطار حوكمة قوي لأمن المعلومات.

## منهجية الدورة التدريبية:



المتدربون من خلال مصممة لربط المفاهيم القانونية بالواقع التقني تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، مؤسسات بسبب انتهاكات أمنية، وورش العمل دراسات الحالة الواقعية لغرامات قانونية فرضت على لأمن المعلومات. سيتمكن التحقيقات تتوافق مع القوانين. تتضمن المنهجية مناقشات متعمقة التطبيقية، من فهم كيفية صياغة سياسات أمنية مجرد إجراء واحدة يقدم الجنائية الرقمية. سيتم التركيز على تحقيق الامتثال حول التحديات القانونية للأمن السحابي قانونياً المؤسسات من بناء بيئة رقمية آمنة وممتثلة هذه الدورة لتمكين BIG BEN Training Center كعملية مستمرة، وليس

## خريطة المحتوى التدريبي (محاور الدورة التدريبية):

### الوحدة الأولى: أساسيات الأمن القانوني للبيانات

- مقدمة إلى قوانين حماية البيانات والخصوصية.
- الفرق بين الأمن السيبراني والامتثال القانوني.
- أهمية الامتثال لتجنب العقوبات والمخاطر.
- التشريعات الدولية الرئيسية (GDPR, CCPA).
- التشريعات المحلية وقوانين الأمن السيبراني.
- مفاهيم البيانات الشخصية والبيانات الحساسة.
- الحقوق والالتزامات بموجب قوانين حماية البيانات.

### الوحدة الثانية: إطار الحوكمة والأمن



- بناء إطار حوكمة لأمن المعلومات<sup>١</sup>
- وضع السياسات والإجراءات الأمنية<sup>١</sup>
- دور مسؤول حماية البيانات<sup>٢</sup> (DPO)
- إدارة المخاطر الأمنية من منظور قانوني<sup>١</sup>
- التدقيق الأمني والامتثال<sup>١</sup>
- تكامل الأمن السيبراني في استراتيجية الأعمال<sup>١</sup>
- تحديد الأدوار والمسؤوليات<sup>١</sup>

## الأمنية الوحدة الثالثة: الامتثال القانوني في الممارسات

- متطلبات التشفير وتخزين البيانات<sup>١</sup>
- تأمين الوصول إلى البيانات الحساسة<sup>١</sup>
- التعامل مع سجلات المراقبة والبيانات<sup>١</sup>
- أمن العقود الرقمية والتوقيع الإلكتروني<sup>١</sup>
- الامتثال في الخدمات السحابية وموردي الطرف الثالث<sup>١</sup>
- حماية الملكية الفكرية الرقمية<sup>١</sup>
- أمن البريد الإلكتروني والاتصالات<sup>١</sup>

## الوحدة الرابعة: الاستجابة للحوادث من منظور قانوني

- تطوير خطة الاستجابة للحوادث الأمنية<sup>١</sup>
- التنظيمية<sup>١</sup> الإبلاغ عن انتهاكات البيانات إلى الجهات
- التعامل مع حوادث الأمن وفقاً للقانون<sup>١</sup>
- التحقيقات الجنائية الرقمية وجمع الأدلة<sup>١</sup>
- التواصل مع العملاء بعد وقوع حادث<sup>١</sup>
- تجنب المسؤولية القانونية في حالة الحوادث<sup>١</sup>
- التعافي القانوني بعد وقوع الحادث<sup>١</sup>



## الوحدة الخامسة: مستقبل التشريعات والأمن السيبراني

- التشريعات الناشئة في مجال الذكاء الاصطناعي<sup>١</sup>.
- الامتثال في عالم إنترنت الأشياء (IoT)<sup>٢</sup>.
- تحديات الأمن القانوني في العملات الرقمية<sup>١</sup>.
- دور الذكاء الاصطناعي في الامتثال<sup>١</sup>.
- التعاون بين الإدارة القانونية والأمن السيبراني<sup>١</sup>.
- المرونة القانونية في بيئة الأعمال المتغيرة<sup>١</sup>.
- تأثير الأمن القانوني على الابتكار<sup>١</sup>.

### الأسئلة المتكررة:

## التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة<sup>١</sup>.

## الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

إجمالي المدة إلى بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. ٢٥-٣٠ راحة وأنشطة تفاعلية<sup>١</sup> ليصل

### سؤال للتأمل:



على مجرد الامتثال للوائح كيف يمكن للمؤسسات أن تبتكر إطاراً قانونياً في ظل التطور السريع للتقنيات والتشريعات الرقمية،  
قصوى المؤسسة من التكيف مع التغييرات القانونية الحالية، بل ينشئ ثقافة حوكمة استباقية، ويمكن وأمنياً لا يقتصر  
لتعزيز الثقة والنمو المستدام؟ المستقبلية، ويضمن حماية البيانات كأولوية

## ما الذي يميز هذه الدورة عن غيرها من الدورات؟

لدمج هذين المجالين الأمن السيبراني والتشريعات القانونية، مما يوفر تميز هذه الدورة بتركيزها المتخصص على التقاطع بين  
التطبيق العملي لتحقيق الامتثال، من صياغة القوانين. بدلاً من تناول كل مجال على حدة، نغوص في محتوى مصمماً خصيصاً  
مع تحليل مفصل قانوني. تقدم الدورة دراسات حالة واقعية لانتهاكات السياسات الأمنية إلى التعامل مع الحوادث من منظور  
المؤسسة من حماية أصولها الرقمية مع لنتائجها وكيفية تجنبها. نركز على بناء إطار حوكمة بيانات أدت إلى عواقب قانونية،  
في إطار نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء الالتزام الكامل بالقوانين. إنها ليست مجرد دورة قوي يمكن  
قانوني سليم. متخصصين في الأمن قادرين على العمل