CONCEPT

القانون السيبراني وقانون تقنية المعلومات: الجرائم المعلوماتية والأدلة الإلكترونية ومسؤولية المنصات

21 – 25 فبراير 2027

الدمام - فندق خمس نجوم في المنطقة الشرقية



القانون السيبراني وقانون تقنية المعلومات: الجرائم المعلوماتية والأدلة الإلكترونية ومسؤولية المنصات

المرجع: 19423_743 **التاريخ:** 21 – 25 فبراير 2027 **المكان:** الدمام - فندق خمس نجوم في المنطقة الشرقية **الرسوم:** SAR 19500

مقدمة:

حين تتعرض المنظمة لبرمجية فدية أو تسريب لملف العملاء أو حساب مزيف باسم أحد التنفيذيين، تتسارع الأسئلة القانونية أكثر مما تستطيع الإدارة الإجابة عنه: ما الجريمة المعلوماتية التي وقعت، وهل تنكشف الشركة نفسها، وأي الأدلة الإلكترونية يجب حفظها سليمة، ومن يجب إخطاره، وأي اختصاص قضائي ينطبق. تمنح هذه الدورة من كور كونسبت المستشارين القانونيين داخل المنشآت وموظفي الامتثال وحوكمة تقنية المعلومات فهما تطبيقيا للقانون السيبراني وقانون تقنية المعلومات، من فئات الجرائم المعلوماتية إلى مسؤولية المنصات والتعاون الدولي. ويعد المشاركون مذكرة الاستجابة القانونية للحادث السيبراني لحالة اختراق دراسية.

أهداف الدورة:

- تكييف الحادث وفق فئات الجرائم المعلوماتية: الدخول غير المشروع والاعتراض والمساس بالبيانات والأنظمة وإساءة استخدام الأجهزة والتزوير والاحتيال المعلوماتي
- تقدير انكشاف الشركة جنائيا ومدنيا الناتج عن تصرفات الموظفين والمتعاقدين والأطراف الثالثة عبر الإنترنت
- تقديم المشورة بشأن قبول السجلات الإلكترونية وسلامتها وسلسلة حيازتها في النزاعات والدعاوى الجزائية
- تطبيق شروط الإعفاء الممنوح للوسطاء وإجراء الإشعار والإزالة على المحتوى المستضاف وأسماء النطاقات والمنتجات البرمجية
- تحديد واجبات الإخطار عن الحوادث والاختصاص العابر للحدود ومسارات التعاون وفق Convention on Cybercrime Budapest
- صياغة مذكرة الاستجابة القانونية للحادث السيبراني بما تتضمنه من جرائم وانكشاف وخطوات حفظ الأدلة وإخطارات وإجراءات موصى بها

الفئة المستهدفة:

- الإدارات القانونية داخل المنشآت التي تشير على الإدارة في الحوادث السيبرانية وسوء السلوك عبر الإنترنت والنزاعات التقنية
- إدارات الامتثال المسؤولة عن الإبلاغ عن الاختراقات والمراسلات الرقابية وإنفاذ السياسات
- إدارات حوكمة تقنية المعلومات وسياسات أمن المعلومات التي تضع قواعد الاستخدام المقبول والمراقبة والحوادث
- إدارات المخاطر والمراجعة الداخلية التي تقيم الانكشاف القانوني الناتج عن العمليات التقنية والموردين
- مديرو المنصات الرقمية والمنتجات الذين يستضيفون محتوى المستخدمين أو يديرون أسماء النطاقات أو يطرحون برمجيات مرخصة

محاور الدورة:

اليوم 1: نطاق القانون السيبراني وقانون تقنية المعلومات ومشهد الجرائم المعلوماتية

- خريطة نطاق قانون تقنية المعلومات: الجرائم المعلوماتية والأدلة الإلكترونية والوسطاء والنطاقات والبرمجيات
- تعريفات بيانات الحاسوب والنظام المعلوماتي وبيانات الحركة في الصكوك الدولية لمكافحة الجرائم المعلوماتية
- المسار الجزائي مقابل المسار المدني في الأفعال الضارة عبر الإنترنت: مصفوفة اختيار وسيلة الانتصاف
- سجل الانكشاف القانوني للحوادث السيبرانية في منظمة متعددة الأنشطة
- مراجعة الوضع الحالي لسياسات الاستخدام المقبول والمراقبة والإبلاغ عن الحوادث

اليوم 2: فئات الجرائم المعلوماتية ومسؤولية الشركات

- بنية الجرائم في Budapest Convention اتفاقية بودابست بشأن الجريمة الإلكترونية: الدخول غير المشروع والاعتراض غير المشروع والمساس بالبيانات
- المساس بالأنظمة وإساءة استخدام الأجهزة: القصد والتفويض والاستثناءات
- اختبار أركان التزوير المعلوماتي والاحتيال المعلوماتي وانتحال الهوية
- جرائم التشهير والمضايقة عبر الإنترنت: النشر وتحديد المعني وأوجه الدفاع
- نموذج مسؤولية الشركات: إسناد أفعال الموظفين وقصور الإشراف والجزاءات

اليوم 3: الأدلة الإلكترونية وحماية السجلات وسلسلة الحيازة

- اختبارات قبول السجلات الإلكترونية: الأصالة والسلامة وقاعدة الدليل الأفضل
- سجل سلسلة الحيازة: الجمع والتحقق بقيم التجزئة والتخزين وسجلات النقل
- إشعار التجميد لأغراض التقاضي وطلب حفظ السجلات وصناديق البريد والبيانات السحابية
- حماية المستندات الإلكترونية: سبل الانتصاف من التعديل والإتلاف والإفشاء غير المصرح به
- إجراءات الحفظ العاجل وأوامر التقديم في Budapest Convention

اليوم 4: مسؤولية الوسطاء وأسماء النطاقات والبرمجيات وواجبات الإخطار

- شروط الإعفاء الممنوح للوسطاء في خدمات النقل المجرد والتخزين المؤقت والاستضافة
- مسار الإشعار والإزالة: صحة الإشعار والإشعار المضاد وسجلات المخالفين المتكررين
- نزاعات أسماء النطاقات: السطو على النطاقات والتسجيل بسوء نية ومسار الشكوى الإدارية
- مسؤولية تراخيص البرمجيات: إخلاء الضمان ودعاوى العيوب وسبل معالجة مخالفة الترخيص
- مصفوفة واجبات الإخطار عن الحوادث: الجهات الرقابية وأصحاب البيانات والأطراف المتعاقدة وشركات التأمين

اليوم 5: القضايا العابرة للحدود ومذكرة الاستجابة القانونية للحادث السيبراني

- جدول تحليل الاختصاص: موقع الخادم والمجني عليه والجاني والبيانات
- المساعدة القانونية المتبادلة ومسار الإحالة إلى شبكة الاتصال على مدار الساعة في Budapest Convention
- مراجعة ملف الاختراق الدراسي: اختراق البريد الإلكتروني للأعمال لدى شركة خدمات لوجستية
- صياغة مذكرة الاستجابة القانونية للحادث السيبراني: الجرائم والانكشاف والأدلة والإخطارات
- لجنة المراجعة القانونية: الدفاع عن المذكرة وأسئلة المساءلة وأولويات العمل

المهارات التي ستكتسبها:

- تكييف الجرائم المعلوماتية
- تقدير المسؤولية السيبرانية للشركات
- فحص قبول الأدلة الإلكترونية
- توثيق سلسلة الحيازة
- تحليل إعفاءات الوسطاء
- معالجة نزاعات أسماء النطاقات
- تخطيط الإخطار عن الاختراقات
- تحديد الاختصاص العابر للحدود

لماذا تحضر هذه الدورة:

- العودة بنموذج مذكرة الاستجابة القانونية للحادث السيبراني مجرب على ملف اختراق واقعي
- تزويد الإدارة بموقف قانوني واضح خلال ساعات من وقوع الحادث دون انتظار المستشار الخارجي
- الحفاظ على صلاحية السجلات الإلكترونية أمام المحاكم بتحديد خطوات الحفظ القانوني قبل إعادة بناء الأنظمة
- مقارنة ممارسات القانون السيبراني مع زملاء من الشؤون القانونية والامتثال والحوكمة في البنوك والخدمات اللوجستية والتجزئة والاتصالات والخدمات العامة

الخاتمة:

يتحول الحادث السيبراني إلى مسألة قانونية منذ لحظة سرقة البيانات أو تعديلها أو نشرها. ينتقل الأسبوع من نطاق قانون تقنية المعلومات وفئات الجرائم المعلوماتية، مرورا بمسؤولية الشركات والقواعد القانونية للأدلة الإلكترونية وسلسلة الحيازة، ثم إعفاءات الوسطاء والإشعار والإزالة ونزاعات أسماء النطاقات ومسؤولية البرمجيات وواجبات الإخطار، وصولا إلى الاختصاص العابر للحدود والتعاون وفق Budapest Convention. وينتهي اليوم الأخير بمذكرة استجابة قانونية جاهزة للاستخدام. تغطي الدورة المبادئ العامة ولا تعد استشارة قانونية.