مقدمة:

مع تزايد الاعتماد على التقنيات الرقمية في مختلف قطاعات العمل، وارتفاع حجم تداول البيانات الشخصية بين الأفراد والمؤسسات، أصبحت حماية هذه البيانات من أبرز التحديات القانونية والتنظيمية في العصر الحديث. ونتيجة لهذا التحول، بات من الضروري أن تمتلك المؤسسات فهماً دقيقاً للإطار القانوني الذي ينظم حماية البيانات الشخصية، لضمان الامتثال للأنظمة وتحقيق الحوكمة الفعالة للمعلومات.

تهدف هذه الدورة التدريبية إلى تزويد المشاركين بمعرفة متعمقة حول الإطار القانوني الناظم لحماية البيانات الشخصية، من خلال استعراض المبادئ القانونية الأساسية، والتشريعات المحلية والدولية ذات الصلة، مع التركيز على الأنظمة المطبقة في المملكة العربية السعودية والأنظمة العالمية مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR).

تتناول الدورة الجوانب التنظيمية والتقنية التي تكفل الامتثال لنظام حماية البيانات، وتسهم في بناء فهم متكامل للمسؤوليات القانونية الواقعة على عاتق المؤسسات والأفراد في إدارة البيانات. كما تقدم تدريباً متخصصاً في كيفية معالجة البيانات بما يتوافق مع الضوابط القانونية والسياسات المؤسسية المعتمدة، وذلك من خلال الجمع بين المعرفة النظرية والتطبيق العملي.

تركز الدورة أيضاً على التحديات العملية المرتبطة بتطبيق النظام، مثل آليات الإفصاح، تقديم التقارير، الاستجابة للجهات الرقابية، والعقوبات القانونية المحتملة في حال المخالفات، مما يساعد المشاركين على تبني إجراءات وقائية واستباقية تضمن الامتثال المستدام وتعزز الثقة المؤسسية.

الفئات المستهدفة:

تم تصميم هذه الدورة لتخاطب فئات مهنية متعددة، تشمل:

- المسؤولين عن الامتثال والرقابة القانونية داخل المؤسسات.
- موظفي الشؤون القانونية ومكاتب المستشارين القانونيين.
- خبراء أمن المعلومات والمتخصصين في حماية الخصوصية.
- مسؤولي نظم وتقنية المعلومات في الشركات والمؤسسات.
- العاملين في قطاع الاتصالات والخدمات الرقمية.
- موظفي الموارد البشرية وإدارات شؤون الموظفين.
- المختصين في تحليل البيانات والتعامل مع المعلومات الحساسة.
- مدراء المشاريع التقنية ممن يتعاملون مع البيانات الرقمية.
- المحامين والمستشارين القانونيين العاملين في قضايا حماية البيانات.
- الأفراد المهتمين بالتخصص في مجال حماية البيانات والامتثال التنظيمي.

الكفاءات المستهدفة:

من خلال المشاركة في هذه الدورة، سيكتسب المتدربون الكفاءات المهنية التالية:

- الإلمام الكامل بالتشريعات القانونية ذات الصلة بحماية البيانات الشخصية.
- القدرة على تحليل القواعد التنظيمية التي تحكم إدارة البيانات.
- تطبيق الإجراءات القانونية لحماية الخصوصية في البيئات الرقمية.
- صياغة سياسات مؤسسية متوافقة مع الإطار القانوني المحلي والدولي.
- التحقق من مدى التزام المؤسسات بنظام حماية البيانات.
- اتخاذ قرارات قانونية مدروسة تتعلق بمعالجة البيانات.
- إعداد تقارير الامتثال القانونية وفق المتطلبات الرسمية.
- إدارة العلاقة مع الجهات الرقابية المعنية بحماية البيانات.
- التمكن من تقييم المخاطر القانونية المرتبطة بالبيانات وتطوير استجابات فعالة.
- تعزيز القدرة المؤسسية على التعامل مع المعلومات الشخصية بحرفية ومهنية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المشاركون قادرين على:

- توضيح المبادئ القانونية الأساسية المتعلقة بحماية البيانات الشخصية.
- تحديد المسؤوليات القانونية الملقاة على المؤسسات عند التعامل مع البيانات.
- التمييز بين أنواع البيانات الشخصية والبيانات الحساسة، والضوابط القانونية المرتبطة بها.
- تحليل الأنظمة المحلية والدولية، وتقييم أوجه الالتقاء والاختلاف فيما بينها.
- شرح الإجراءات التنظيمية المتعلقة بجمع، تخزين، معالجة، ونقل البيانات.
- إعداد وصياغة السياسات المؤسسية لحماية البيانات بطريقة قانونية ودقيقة.
- تقييم احتمالات اختراق البيانات وتحديد التدابير القانونية الوقائية المناسبة.
- بناء آليات شفافية فعالة لإعلام المستخدمين بحقوقهم وتقديم الإفصاحات اللازمة.
- ربط حماية البيانات الشخصية بمنظومة الحوكمة المؤسسية والامتثال التنظيمي العام.
- إعداد تقارير الامتثال بما يتفق مع متطلبات السلطات الرقابية.
- شرح كيفية تقديم الشكاوى والتعامل مع المخالفات النظامية.
- تصميم خطة عمل مؤسسية تضمن الامتثال المستمر والمستدام لنظام حماية البيانات.
- استخدام النماذج القانونية المعتمدة لصياغة السياسات والإجراءات ذات العلاقة.
- التدقيق القانوني على البيانات وممارسات المؤسسة في إدارتها.
- مراقبة الأداء المؤسسي بشكل دوري وتحديث السياسات استناداً للتغييرات القانونية.

محتوى الدورة التدريبية:

الوحدة الأولى: الإطار العام لحماية البيانات الشخصية

- تعريف البيانات الشخصية والتمييز بينها وبين البيانات الحساسة.
- المفهوم القانوني لحماية الخصوصية في البيئة الرقمية الحديثة.
- الدوافع التي أدت إلى سن أنظمة لحماية البيانات.
- استعراض شامل للأنظمة العالمية مثل GDPR، ومقارنتها بالتشريعات المحلية في المملكة العربية السعودية.
- المبادئ الأساسية لحماية البيانات: الشفافية، العدالة، المساءلة.
- العلاقة بين حماية البيانات والأمن السيبراني.
- مسؤولية الدولة في تنظيم وحوكمة البيانات على المستوى الوطني.

الوحدة الثانية: المسؤوليات القانونية والمؤسسية

- تحديد المسؤوليات داخل المؤسسة بشأن معالجة البيانات.
- حقوق الأفراد وواجبات المؤسسات تجاهها.
- الصياغة القانونية لإشعارات الخصوصية وآليات الحصول على الموافقة.
- الإجراءات النظامية الواجب اتباعها عند حدوث خرق أو تسريب للبيانات.
- دور مسؤول حماية البيانات (DPO) والمتطلبات القانونية لتعيينه.
- سياسات الحذف الآمن وتقييد المعالجة.
- تنظيم العقود مع مزودي الخدمة الخارجيين.
- تطبيق مبدأ تقليل البيانات وتقليل مدة الاحتفاظ بها إلى الحد الأدنى اللازم.

الوحدة الثالثة: الامتثال والرقابة والتقارير

- معايير ومتطلبات الامتثال لنظام حماية البيانات الشخصية.
- إعداد تقارير الامتثال وتقديمها للجهات المختصة.
- إدارة المخاطر القانونية المرتبطة بمعالجة البيانات.
- آليات التدقيق القانوني والرقابة الداخلية.
- الاستجابة للطلبات القانونية من الأفراد وأصحاب الحقوق.
- تصميم خطط امتثال شاملة للمؤسسة وتحديثها باستمرار.
- أدوات وآليات الرقابة التقنية والقانونية على البيانات.
- رصد الإخفاقات التنظيمية وتطوير الحلول المناسبة.

الوحدة الرابعة: الحقوق الفردية وحماية الخصوصية

- الحقوق القانونية لأصحاب البيانات بموجب الأنظمة المعتمدة.
- آلية تقديم الشكاوى واستلام ومعالجة الطلبات.

- الحق في الوصول والنقل والتصحيح والاعتراض على المعالجة.
- إدارة البيانات بما يتوافق مع مبدأ احترام الخصوصية.
- توظيف التقنيات الحديثة لدعم الحقوق القانونية للأفراد.
- تحليل حالات واقعية تمثل انتهاكات لحقوق حماية البيانات.
- إعداد النماذج والإشعارات القانونية لتوثيق الحقوق الفردية.
- التعامل مع طلبات الحذف والتقييد وفق الإطار القانوني.

الوحدة الخامسة: الممارسات العملية وأفضل التطبيقات

- صياغة سياسات الخصوصية المؤسسية بطريقة متوافقة مع القوانين.
- تصميم العمليات المؤسسية لضمان الامتثال الكامل للنظام.
- تطوير خطة استجابة للطوارئ في حال حوادث تسريب البيانات.
- تدريب الموظفين على التزاماتهم القانونية في حماية البيانات.
- دمج مبادئ الحماية في دورة حياة الأنظمة التقنية.
- متابعة التطورات التشريعية والإدارية في مجال حماية البيانات.
- التعاون مع الجهات التنظيمية لبناء ثقافة امتثال راسخة.
- تطبيق أدوات تقييم الأثر لحماية البيانات (DPIA).
- رسم خارطة تدفق البيانات لتحديد مصادر البيانات وتقييم المخاطر.

خلاصة وتوصيات الدورة التدريبية:

تُعد حماية البيانات الشخصية من الأولويات القانونية للمؤسسات في البيئة الرقمية المعاصرة، ويُشكل الإطار القانوني لنظام حماية البيانات حجر الأساس في ضمان التزام المؤسسات بمعايير الخصوصية والشفافية. تسهم هذه الدورة في رفع الوعي القانوني وبناء قدرات عملية تمكّن المشاركين من تطبيق مبادئ النظام بكفاءة. ومن الضروري أن تواصل المؤسسات مراجعة سياساتها وإجراءاتها بانتظام لمواكبة التحديثات التشريعية والتقنية، مع تبني نهج وقائي يجمع بين الحوكمة القانونية والتقنيات الحديثة لضمان حماية فعّالة ومستدامة للبيانات الشخصية.