مقدمة:

في ظل التوسع الرقمي المتسارع الذي يشهده العالم اليوم، أصبحت حماية الخصوصية والبيانات الشخصية للأفراد من أهم القضايا القانونية والأخلاقية التي تواجه الأفراد والمؤسسات على حد سواء. تفرض البيئة التقنية الراهنة التزامات دقيقة ومتزايدة على الجهات التي تتولى جمع أو معالجة أو تخزين بيانات الأفراد، وهو ما جعل من الامتثال لمعايير حماية البيانات مطلبًا أساسيًا لتحقيق الثقة والاستدامة.

تهدف هذه الدورة التدريبية إلى تزويد المشاركين بفهم شامل ومتكامل للجوانب القانونية والتنظيمية المرتبطة بحقوق الأفراد في الخصوصية وحماية بياناتهم، مع التركيز على الإجراءات العملية والمعايير الفنية والقانونية التي تكفل الامتثال الكامل للتشريعات المحلية والدولية ذات الصلة.

كما تسلط الدورة الضوء على أفضل الممارسات المتبعة في التعامل مع البيانات الشخصية الحساسة بطريقة قانونية وآمنة، وتوضح كيفية إدارة المخاطر المرتبطة بالتسريبات والانتهاكات المحتملة للخصوصية. وتسعى كذلك إلى إعداد كوادر مؤسسية تتمتع بالكفاءة والمعرفة في مجال الحقوق الرقمية، وتعزيز ثقافة مؤسسية قائمة على احترام الخصوصية كأحد أسس الثقة بين المؤسسة وأصحاب البيانات.

الفئات المستهدفة:

تستهدف هذه الدورة جميع الأفراد المعنيين بحماية البيانات والخصوصية داخل المؤسسات، بما يشمل:

- موظفي أقسام تقنية المعلومات.
- العاملين في مجالات الامتثال والحوكمة المؤسسية.
- موظفي الموارد البشرية الذين يتعاملون مع بيانات الموظفين والمستخدمين.
- مسؤولي حماية البيانات المعتمدين في المؤسسات.
- القانونيين والمستشارين المتخصصين في الخصوصية والبيانات.
- خبراء التسويق الرقمي والتحليلات التقنية.
- مسؤولي أمن المعلومات ومدراء الأمن السيبراني.
- مدراء نظم وقواعد البيانات.
- مطوري الأنظمة الرقمية ومنصات التطبيقات.
- الباحثين المهتمين بقضايا الخصوصية والحقوق الرقمية.
- الموظفين الجدد في الشركات المعتمدة على البيانات.
- رواد الأعمال وأصحاب المشاريع التقنية الناشئة.

الكفاءات المستهدفة:

من خلال المشاركة في هذه الدورة، سيكتسب المتدربون مجموعة من الكفاءات الأساسية في مجال حماية البيانات، أبرزها:

- القدرة على التحليل القانوني للبيانات الشخصية وأنماط استخدامها.
- تطوير سياسات متكاملة لحماية الخصوصية داخل المؤسسات.

- إدارة متطلبات الامتثال التنظيمي وفقًا لأطر الحوكمة الرقمية.
- التعرف على الممارسات الآمنة وغير الآمنة في التعامل مع البيانات.
- إعداد وصياغة أطر قانونية لحماية الحقوق الرقمية للأفراد.
- إدارة ومواجهة مخاطر تسرب البيانات والانتهاكات الإلكترونية.
- إعداد تقارير رقابية وتوثيقية لعمليات الامتثال المؤسسي.
- تقييم فعالية أنظمة حماية الخصوصية من الناحية الفنية.
- التمييز بين الأدوار والمسؤوليات بين جهات المراقبة والمعالجة.
- تطبيق معايير الوصول الآمن والتحكم بالأنظمة الرقمية.
- دمج متطلبات الخصوصية ضمن دورة حياة الأنظمة والتطبيقات.

الأهداف التدريبية:

عند إتمام الدورة، سيكون المشاركون قادرين على:

- فهم المفاهيم الأساسية للخصوصية وحماية البيانات الشخصية.
- تحليل الإطار القانوني المحلي والدولي المنظم لحقوق الأفراد في البيانات.
- تفسير المبادئ الأخلاقية والمهنية المتعلقة بإدارة المعلومات الشخصية.
- تقييم مدى توافق المؤسسات مع متطلبات التشريعات الحديثة في حماية البيانات.
- تطبيق أفضل الممارسات في جمع ومعالجة وتخزين البيانات الشخصية بطريقة آمنة.
- تصميم سياسات خصوصية مؤسسية تتوافق مع القوانين والمعايير التنظيمية.
- استخدام أدوات تقييم المخاطر الخاصة بانتهاكات الخصوصية.
- إعداد تقارير امتثال شاملة لعرضها على الجهات الرقابية المختصة.
- التمييز بين أنواع البيانات الشخصية (العامة، الحساسة، المجهولة).
- صياغة إجراءات فعالة للتعامل مع حوادث اختراق البيانات.
- تطوير مهارات التواصل والتوعية بأهمية حماية الخصوصية في بيئة العمل.
- تعزيز ثقافة الخصوصية داخل المؤسسة من خلال التدريب والتوعية المستمرة.
- تطبيق أدوات التحكم في الوصول إلى البيانات ضمن الأنظمة الرقمية.
- تفسير العقود والمسؤوليات بين جهات التحكم والمعالجة.
- مراقبة وتوثيق الأنشطة والعمليات المؤثرة على خصوصية المستخدمين.

محتوى الدورة التدريبية:

الوحدة الأولى: مدخل إلى الخصوصية وحماية البيانات الشخصية

- التعريف بمفهوم الخصوصية وأهميتها في العصر الرقمي.
- الفروق بين مفهومي الخصوصية وحماية البيانات.
- أنواع البيانات: الشخصية، الحساسة، والمجهولة.
- مراحل دورة حياة البيانات داخل المؤسسات.
- أهمية الحصول على موافقة صريحة ومسبقة من الأفراد.
- مبادئ الشفافية والمساءلة في التعامل مع البيانات.
- التعرف على الفاعلين في منظومة حماية البيانات (الجهة المراقبة، المعالجة).
- أثر الخصوصية في بناء الثقة بين المؤسسة والمستفيدين.
- العلاقة التبادلية بين حماية الخصوصية والأمن السيبراني.

الوحدة الثانية: الأطر القانونية والتنظيمية لحماية البيانات

- نظرة على التشريعات المحلية (مثل قوانين حماية البيانات الوطنية).
- المبادئ الأساسية للائحة حماية البيانات الأوروبية (GDPR).
- مقارنة تشريعية بين الأنظمة المحلية والدولية.
- استعراض حقوق الأفراد القانونية وفق أحدث التشريعات.
- التزامات المؤسسات وجهات المعالجة بموجب القوانين.
- العقوبات القانونية في حال عدم الامتثال للتشريعات.
- مفهومي الخصوصية حسب التصميم وحسب الإعداد الافتراضي.
- التزامات التوثيق وتسجيل الأنشطة المرتبطة بالبيانات.
- دور الجهات الرقابية والمؤسسات التنظيمية في فرض الامتثال.

الوحدة الثالثة: الإدارة القانونية والأمنية للبيانات

- آليات تصنيف البيانات وتصميم آليات حماية مناسبة.
- صياغة سياسات خصوصية واضحة وشفافة.
- إعداد نماذج الموافقة والبيانات القانونية للمعالجة.
- حماية البيانات من خلال العقود واتفاقيات الخدمة.
- استخدام أدوات التشفير وتأمين البيانات أثناء التخزين والنقل.
- التحكم في الوصول إلى البيانات الحساسة وفق الصلاحيات.
- تقييم الأثر على الخصوصية قبل تنفيذ مشاريع تقنية (PIA).
- وضع خطط استجابة لانتهاكات البيانات وحوادث الاختراق.
- تدريب الموظفين على الوعي الأمني وحماية المعلومات.

الوحدة الرابعة: حقوق الأفراد وآليات تقديم الشكاوى

- شرح حقوق الأفراد: الوصول، التصحيح، النقل، الإلغاء.
- سبل تقديم الاعتراضات القانونية على معالجة البيانات.
- كيفية إدارة الطلبات المتعلقة بحقوق الأفراد في المؤسسات.
- بناء آليات فعالة للتعامل مع الشكاوى والتظلمات.
- تحديد المدد الزمنية للرد على الطلبات حسب القانون.
- ضمان الشفافية الكاملة في الإجراءات المتبعة.
- معالجة البيانات المتعلقة بالأطفال وذوي الاحتياجات الخاصة.
- تعزيز التزام المؤسسات بحماية الحقوق الرقمية لجميع المستخدمين.

الوحدة الخامسة: حوكمة البيانات والمسؤولية المؤسسية

- بناء منظومة متكاملة لحوكمة البيانات المؤسسية.
- تعريف مسؤوليات ضابط حماية البيانات (DPO) ودوره المحوري.
- دمج مفاهيم الخصوصية في استراتيجيات التحول الرقمي.
- إشراك الإدارة العليا في مبادرات حماية الخصوصية.
- إدراج حماية البيانات ضمن نظم إدارة الجودة المؤسسية.
- إعداد تقارير دورية لمراجعة الأداء والامتثال.
- إجراء تدقيقات داخلية وخارجية لضمان سلامة الأنظمة.
- مواكبة التغيرات التشريعية والتقنية في مجال حماية البيانات.
- ترسيخ ثقافة تنظيمية قائمة على احترام الخصوصية والمسؤولية الرقمية.

الخلاصة والتوصيات:

تسلط هذه الدورة الضوء على البعد القانوني والأخلاقي لمسألة الخصوصية الرقمية، وتوضح ضرورة التزام المؤسسات والممارسين بالمعايير والتشريعات ذات الصلة. تمثل حماية الخصوصية عنصرًا أساسيًا لبناء الثقة وتعزيز المصداقية والامتثال في العصر الرقمي. ويوصى بأن تقوم المؤسسات بمراجعة وتحديث سياساتها بشكل دوري، إلى جانب توفير برامج تدريب مستمرة لموظفيها لضمان بناء ثقافة تنظيمية واعية بقيمة وأهمية خصوصية البيانات.