

مقدمة:

مع التسارع الكبير في مسار التحول الرقمي داخل المملكة العربية السعودية، برزت الحاجة الملحة إلى وضع أطر تنظيمية وقانونية تُعنى بحماية خصوصية الأفراد وبياناتهم الشخصية، بما يضمن التعامل معها وفق ضوابط واضحة ومعايير عالية من الأمان. ويُعد **نظام حماية البيانات السعودي** من أهم المبادرات التشريعية التي تهدف إلى تنظيم عمليات جمع ومعالجة وتخزين البيانات الشخصية، لا سيما في ظل الاعتماد المتزايد على الحلول الرقمية والتقنيات المتقدمة في مختلف القطاعات.

تهدف هذه الدورة التدريبية إلى تزويد المشاركين بفهم شامل ومتكامل لنظام حماية البيانات السعودي، من خلال التطرق إلى المبادئ الأساسية التي يقوم عليها، واستعراض التزامات الجهات المعنية بمعالجة البيانات، والحقوق المقررة لأصحاب البيانات، إضافة إلى الآليات القانونية المقررة للتفتيش وفرض العقوبات في حالات المخالفة.

كما تسلط الدورة الضوء على الأدوار التنظيمية والإشرافية للهيئات ذات العلاقة، وفي مقدمتها **الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)**، وتناقش أبرز التحديات التي تواجه المؤسسات في تطبيق النظام ضمن بيئة الأعمال الحديثة. تم تصميم الدورة لتكون مرجعًا عمليًا واحترافيًا لجميع المهنيين الذين يتعاملون مع البيانات الشخصية في مؤسساتهم، بغرض رفع مستوى الامتثال وضمان الحماية القانونية للبيانات.

الفئات المستهدفة:

تستهدف دورة "الأنظمة الوطنية كنظام حماية البيانات السعودي" مجموعة واسعة من المهنيين، بما في ذلك:

- مسؤولو الامتثال وحوكمة البيانات داخل المؤسسات.
- المختصون في الأمن السيبراني وتحليل وإدارة المخاطر.
- العاملون في مجالات تقنية المعلومات وإدارة نظم البيانات.
- المستشارون القانونيون المتخصصون في خصوصية البيانات.
- مطورو البرمجيات ومهندسو النظم الرقمية.
- موظفو القطاعات الحساسة كالصحة، المالية، والتعليم.
- مسؤولو حماية البيانات على مستوى المؤسسات الحكومية والخاصة.
- القادة التنفيذيون ومديرو التحول الرقمي.
- طلاب وخريجو تخصصات القانون، نظم المعلومات، وهندسة البرمجيات.
- المهتمون بالأنظمة الوطنية المتعلقة بالقوانين الرقمية وخصوصية البيانات.

أهداف الدورة التدريبية:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- استيعاب المبادئ الأساسية التي يقوم عليها نظام حماية البيانات السعودي.
- فهم الحقوق النظامية الممنوحة لأصحاب البيانات والآليات الكفيلة بحمايتها.
- تطبيق متطلبات النظام في بيئة العمل المؤسسي بفعالية وكفاءة.
- تطوير سياسات داخلية تضمن الامتثال الكامل لمواد النظام.
- تحليل الالتزامات الواقعة على عاتق الجهات المعالجة للبيانات الشخصية.
- تعزيز ثقافة الخصوصية والشفافية داخل المؤسسة.
- اكتساب المهارات الضرورية لإدارة بيانات المستخدمين بطريقة قانونية وآمنة.
- التعرف على الإجراءات الواجب اتباعها في حال وقوع حوادث أمنية تتعلق بالبيانات.
- استخدام أدوات التقييم المؤسسي لتوثيق الالتزام وتحديد مكامن الخلل.
- بناء استراتيجيات فعالة لحوكمة البيانات على المستوى المؤسسي.
- تنظيم عمليات استقبال الشكاوى ومعالجتها وفقاً لمتطلبات النظام.
- إعداد تقارير داخلية وخارجية تعكس مدى التزام المؤسسة بالنظام الوطني.
- إجراء مقارنة موضوعية بين النظام السعودي والأنظمة العالمية المماثلة كـ GDPR.
- تهيئة بيئة عمل متوافقة مع متطلبات الخصوصية الرقمية بشكل مستدام.

الكفاءات المستهدفة:

سيتمكن المشاركون من تطوير المهارات والكفاءات التالية:

- الإلمام الكامل بالمصطلحات القانونية الواردة في نظام حماية البيانات السعودي.
- القدرة على تفسير النصوص النظامية وتطبيقها بشكل عملي داخل المؤسسة.
- تصميم وتنفيذ سياسة داخلية لحماية البيانات تتماشى مع المعايير الوطنية.
- إدارة الاستجابات القانونية لحالات خرق البيانات.
- تقييم المخاطر المتعلقة بعدم الامتثال ووضع حلول للحد منها.
- إعداد تقارير رسمية دقيقة للجهات التنظيمية المختصة.
- تحليل البيانات الشخصية بطريقة تحترم الخصوصية والضوابط القانونية.
- تطبيق تقنيات حديثة تضمن حماية البيانات أثناء التخزين والمعالجة.
- تمكين المؤسسة من الالتزام الفعّال والمستمر بالنظام الوطني لحماية البيانات.

محتوى الدورة التدريبية:

الوحدة الأولى: فهم نظام حماية البيانات السعودي

- خلفية عن صدور النظام والسياق القانوني والتنظيمي المعاصر.

- أهداف النظام ودوره في تنظيم بيئة البيانات الرقمية داخل المملكة.
- الجهات التنظيمية والإشرافية، وعلى رأسها الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).
- التعريف الدقيق للبيانات الشخصية والحساسة.
- المبادئ الأساسية التي يقوم عليها النظام: مبدأ الغرض، الحد الأدنى، الشفافية، الحماية.
- نطاق تطبيق النظام والفئات والجهات المشمولة به.
- الحقوق القانونية لأصحاب البيانات وآلية ممارستها.
- أوجه التشابه والاختلاف مع الأنظمة العالمية كـ GDPR.
- التحديات الميدانية التي تواجه المؤسسات أثناء التطبيق الفعلي للنظام.

الوحدة الثانية: الحقوق والواجبات النظامية

- توضيح حقوق أصحاب البيانات وفق النظام، مثل: الوصول، التصحيح، الحذف، وتقييد المعالجة.
- آليات تقديم الشكاوى ومعالجة المخالفات.
- ضوابط جمع البيانات ومتطلبات الحصول على الموافقة النظامية.
- التزامات المؤسسات نحو الشفافية والإفصاح عن أساليب المعالجة.
- متى يلزم الحصول على موافقة جديدة؟ وكيفية توثيقها؟
- استخدام الأدوات التقنية لتفعيل الحقوق وضمان الممارسة الفعلية لها.
- ضمانات حماية البيانات من الاستغلال أو التسريب غير المشروع.
- توثيق الأنشطة والمعاملات ذات الصلة بحماية البيانات.

الوحدة الثالثة: الامتثال المؤسسي

- أهمية تعيين مسؤول حماية البيانات (DPO) داخل المؤسسة.
- إعداد سجل تفصيلي لعمليات المعالجة وأغراضها.
- توثيق إجراءات الموافقة ومعايير إثباتها قانونياً.
- إعداد تقييمات تأثير حماية البيانات (DPIA) عند معالجة البيانات عالية الخطورة.
- بناء سياسات خصوصية مؤسسية متكاملة.
- تطوير برامج تدريبية لتعزيز الوعي القانوني لدى فرق العمل.
- التزامات التعاقد مع مقدمي الخدمات الخارجيين وتوثيقها قانونياً.
- مراقبة مدى الالتزام من خلال مؤشرات الأداء القانونية (KPIs).
- التفاعل مع التحديثات النظامية والتعديلات التشريعية.

الوحدة الرابعة: التفتيش والمخالفات والعقوبات

- استعراض العقوبات النظامية المقررة في حال الإخلال بالالتزامات.
- مسؤولية المؤسسة النظامية والإدارية عند وقوع مخالفة.
- الظروف التي تستدعي تحويل العقوبة إلى عقوبة جنائية.
- صلاحيات الجهات الرقابية في التفتيش والتحقيق.

- الإجراءات المتبعة أثناء التفتيش المفاجئ أو الدوري.
- سبل الاعتراض النظامي على العقوبات والغرامات.
- تحليل دراسات حالة فعلية لمخالفات وقعت داخل مؤسسات.
- كيفية تقديم رد رسمي للمؤسسة على نتائج التفتيش.
- تطوير أدوات وقائية لتفادي تكرار المخالفات في المستقبل.

الوحدة الخامسة: حماية البيانات في البيئة الرقمية

- تحديات حماية البيانات في بيئات الحوسبة السحابية.
- المعالجة الآمنة للبيانات في بيئة الذكاء الاصطناعي والتعلم الآلي.
- أهمية تقنيات التشفير والهوية الرقمية في حماية البيانات.
- اعتماد سياسة حماية البيانات "حسب التصميم وحسب الإعداد الافتراضي".
- الربط بين نظام حماية البيانات ونظم أمن المعلومات.
- استعراض أدوات التكنولوجيا المساعدة في الامتثال وحفظ الخصوصية.
- خصوصية البيانات كجزء من خطط التحول الرقمي للمؤسسة.
- حماية بيانات الفئات الحساسة كالأطفال وذوي الإعاقة.
- تصميم خارطة طريق لحوكمة البيانات وضمان الامتثال المستدام.

خلاصة وتوصيات الدورة التدريبية:

توفر هذه الدورة التدريبية إطارًا تطبيقيًا دقيقًا لتنفيذ نظام حماية البيانات السعودي داخل المؤسسات، مستندة إلى مزيج من المعرفة النظامية العميقة والمهارات التطبيقية العملية. ومن خلال ما يتعلمه المشاركون، سيكون بإمكانهم بناء بيئة عمل تراعي الخصوصية وتحترم الحقوق القانونية للأفراد، بما يتماشى مع أفضل الممارسات الوطنية والدولية.

وتوصي الدورة بضرورة متابعة التحديثات التشريعية بشكل دوري، وتفعيل أنشطة الامتثال المؤسسي من خلال تدريب الموظفين، وتطوير السياسات والعمليات بشكل مستمر. كما يُنصح بتكامل الجهود بين الفرق القانونية والتقنية لضمان تطبيق

مت