تشير البيانات الحساسة إلى أي معلومات قد تسبب، ضررًا أو تشكل خطرًا على فرد أو منظمة. يعد تحديد البيانات الحساسة ومعالجتها وحمايتها بشكل صحيح أمرًا بالغ الأهمية لضمان خصوصية الأفراد وأمنهم، والحفاظ على سمعة المؤسسة وثقة العملاء. تتضمن بعض الأمثلة الشائعة للبيانات الحساسة تفاصيل الهوية الشخصية والسجلات المالية والسجلات الصحية والملكية الفكرية والأسرار التجارية والمعلومات التجارية السرية. يمكن أن يؤدي الوصول غير المصرح به للبيانات الحساسة أو الكشف عنها أو إساءة استخدامها إلى سرقة الهوية والخسائر المالية والإضرار بالخصوصية الشخصية، مما يؤثر على الأفراد والمؤسسات المشاركة في هذه البيانات. يعد تحديد البيانات الحساسة الخطوة الأولى نحو إدارتها وحمايتها بشكل فعال. لا يمكن للشركات والأفراد تطوير استراتيجية مناسبة للتعامل مع المعلومات الحساسة دون تحديد الهوية بشكل صحيح. بعض الأسباب الرئيسية لتحديد البيانات الحساسة هي: حماية الخصوصية : يعد تحديد البيانات الحساسة أمرًا بالغ الأهمية لحماية خصوصية الأفراد والحفاظ على ثقتهم. يمكن أن يؤدي التعامل غير الملائم مع البيانات الحساسة أو سوء التعامل معها إلى عواقب سلبية على الأفراد المعنيين، بما في ذلك الخسائر المالية والتمييز والاضطراب العاطفي. الامتثال للوائح حماية البيانات : يجب على المؤسسات تحديد البيانات الحساسة وإدارتها للامتثال لقوانين حماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) قد يؤدي عدم الامتثال لهذه اللوائح إلى فرض غرامات باهظة وعقوبات .(CCPA) وقانون خصوصية المستهلك في كاليفورنيا قانونية وفقدان السمعة. منع الخروقات الأمنية : تحديد البيانات الحساسة يساعد المؤسسات على تنفيذ التدابير الأمنية المطلوبة لحمايتها. من خلال الاعتراف بوجود بيانات حساسة، يمكن للمؤسسة تقييم المخاطر ونقاط الضعف المحتملة، والتأكد من بقاء البيانات آمنة. الحفاظ على السمعة وثقة العملاء : يعد التحديد الصحيح وإدارة البيانات الحساسة أمرًا بالغ الأهمية للحفاظ على سمعة المؤسسة وثقة العملاء. يمكن أن تؤدي الخروقات الأمنية التي تنطوي على بيانات حساسة إلى دعاية سلبية، وإلحاق ضرر طويل الأمد بالعلامة التجارية للمنظمة. الوفاء بالالتزامات التعاقدية : قد يكون لدى المنظمات التي تتعامل مع البيانات الحساسة نيابة عن العملاء أو الشركاء التزامات تعاقدية لحماية هذه البيانات. يعد تحديد البيانات الحساسة أمرًا ضروريًا لتلبية هذه المتطلبات التعاقدية والحفاظ على علاقات عمل صحية. يمكن تصنيف البيانات الحساسة إلى عدة أنواع، يتطلب كل منها إجراءات تتضمن :(PII) معالجة وحماية فريدة. تتضمن بعض الأنواع الشائعة من البيانات الحساسة ما يلي: معلومات التعريف الشخصية البيانات التي يمكن استخدامها لتحديد هوية الفرد، سواء بشكل مباشر أو غير مباشر. ومن الأمثلة على ذلك أرقام الضمان الاجتماعي، وأرقام جواز السفر، المعلومات المالية: تندرج البيانات المتعلقة بالمعاملات والحسابات المالية للفرد أو المنظمة ضمن هذه الفئة. تفاصيل بطاقة الائتمان وأرقام الحسابات المصرفية والبيانات المالية هي بعض الأمثلة. بيانات الرعاية الصحية: تحتوي السجلات الطبية وسجلات الرعاية الصحية على تفاصيل دقيقة حول صحة الفرد وتاريخه الطبي. يتضمن ذلك معلومات التشخيص ونتائج الاختبار وتفاصيل الوصفات الطبية. تحكم الأطر القانونية مثل قانون قابلية نقل التأمين الصحي والمساءلة التعامل مع بيانات الرعاية الصحية. الملكية الفكرية: يجب حماية المعلومات التجارية السرية، مثل الأسرار التجارية (HIPAA) وبراءات الاختراع والمواد المحمية بحقوق الطبع والنشر، للحفاظ على الميزة التنافسية وقيمة المؤسسة. معلومات التوظيف: تتطلب سجلات الموظفين، بما في ذلك تقييمات الأداء وتفاصيل التعويضات والإجراءات التأديبية، يمكن أن يؤدي الوصول غير المصرح به إلى هذه البيانات إلى التمييز والصراعات في مكان العمل. بيانات العملاء: تقوم المؤسسات بجمع بيانات العملاء وتخزينها لأغراض تجارية مختلفة. قد تتضمن هذه المعلومات تفاصيل الاتصال أو سجل الشراء أو التفضيلات. يمكن أن يؤدي الكشف غير المصرح به عن بيانات العميل إلى انتهاك قوانين الخصوصية والإضرار بعلاقات العملاء. يعد فهم هذه الأنواع المختلفة من البيانات الحساسة أمرًا ضروريًا للمؤسسات لإدارة أصول المعلومات الأكثر قيمة وحمايتها بشكل فعال. يتيح تحديد البيانات الحساسة بشكل صحيح للشركات تحديد أولويات الموارد وتنفيذ بروتوكولات أمان البيانات المناسبة عبر عملياتها. تعد إدارة البيانات الحساسة أمرًا بالغ الأهمية للحفاظ على أمن وسلامة المعلومات الهامة. تتضمن العملية العديد من المكونات الأساسية، التي تساعد على ضمان تحديد البيانات الحساسة وحمايتها والتعامل معها بشكل سليم طوال دورة حياتها. تشمل المكونات الرئيسية لإدارة البيانات الحساسة ما يلي: الخطوة الأولى في إدارة البيانات الحساسة هي تحديد المعلومات التي تشكل خطراً على المنظمة أو الأفراد المتأثرين بانتهاكات البيانات المحتملة. يتضمن ذلك تقييم أنواع البيانات التي تعتبر حساسة ثم تحديد موقع هذه البيانات ضمن قواعد البيانات وأنظمة التخزين. يعد الفهم الشامل لموقع وسياق البيانات الحساسة أمرًا حيويًا لوضع التدابير الأمنية. من الضروري تصنيفها حسب مستوى حساسيتها أو مستوى الحماية المطلوبة. تشمل مستويات التصنيف الشائعة العامة

والسرية و السرية للغاية. يساعد هذا التصنيف في تحديد الإجراءات الأمنية المناسبة، مما يجعل تطبيق عناصر التحكم في الوصول والتشفير أسهل لحماية البيانات الحساسة. يعمل تصنيف البيانات أيضًا على تبسيط عمليات إدارة البيانات من خلال تمكين المؤسسات من تصميم استراتيجياتها الأمنية لأنواع محددة من البيانات الحساسة. يعد تنفيذ آليات قوية للتحكم في الوصول عنصرًا حاسمًا في إدارة البيانات الحساسة. ومن خلال تحديد أذونات الوصول وتنفيذها، يمكن للمؤسسات تقييد الوصول إلى البيانات الحساسة على الموظفين المصرح لهم فقط، مما يقلل من مخاطر خروقات البيانات. تتضمن تدابير التحكم في الوصول حيث يتم منح الأذونات بناءً على أدوار المستخدمين، والتحكم في الوصول ،(RBAC) التحكم في الوصول المستند إلى الدور مثل وظيفة الوظيفة أو الموقع أو الوقت الوصول. يعد تخزين البيانات الحساسة بشكل صحيح ،(ABAC) المستند إلى السمات أمرًا بالغ الأهمية للحفاظ على سريتها وسلامتها. تتطلب حلول التخزين الآمن اعتماد تقنيات التشفير المناسبة عندما تكون البيانات في حالة ثبات، مما يضمن استحالة الوصول غير المصرح به. ويجب أيضًا فصل قواعد البيانات، مع عزل البيانات الحساسة عن المعلومات الأقل حساسية أو غير الحساسة لتقليل مخاطر خروقات البيانات. يجب أن تلتزم إدارة البيانات وقانون قابلية نقل ،(GDPR) الحساسة بمختلف قوانين حماية البيانات ولوائح الخصوصية مثل اللائحة العامة لحماية البيانات يتطلب ضمان الامتثال البقاء على .(CCPA) وقانون خصوصية المستهلك في كاليفورنيا ،(HIPAA) التأمين الصحي والمساءلة اطلاع بأحدث المتطلبات القانونية، وإجراء عمليات تدقيق منتظمة، وتحديث سياسات إدارة البيانات وفقًا لذلك. تعد مراقبة وتدقيق عمليات إدارة البيانات الحساسة أمرًا ضروريًا للحفاظ على الشفافية، وضمان الامتثال للوائح المعمول بها. تحدد عمليات التدقيق المنتظمة نقاط الضعف المحتملة، مما يسمح للمؤسسات باتخاذ التدابير التصحيحية وتعديل السياسات الأمنية وفقًا لذلك. استراتيجيات التعامل مع البيانات الحساسة وحمايتها تساعد الاستراتيجيات التالية المؤسسات على التعامل مع البيانات الحساسة وحمايتها بشكل فعال مع الحفاظ على الأمان والامتثال وثقة العملاء: يعد التشفير عنصرًا حاسمًا في حماية البيانات الحساسة. يعمل التشفير على تأمين المعلومات الحساسة سواء أثناء النقل أو أثناء الراحة عن طريق تحويل البيانات إلى تنسيق غير قابل للقراءة ولا يمكن فك تشفيره إلا باستخدام المفتاح الصحيح. من الضروري استخدام خوارزميات تشفير قوية، وتحديث مفاتيح التشفير بانتظام، وتطبيق التشفير الشامل في السيناريوهات التي يجب فيها نقل البيانات بين الأنظمة. جرد البيانات المنتظمة وعمليات التدقيق يساعد إجراء عمليات جرد وتدقيق منتظمة للبيانات المؤسسات على الحفاظ على فهم واضح للبيانات الحساسة التي تمتلكها. تشمل عمليات التدقيق تحديد مصادر البيانات، ومراجعة سياسات تخزين البيانات والتعامل معها، وتقييم فعالية تدابير حماية البيانات الحالية. يتيح التدقيق المنتظم للمؤسسات معالجة نقاط الضعف وضمان الامتثال المستمر للوائح حماية البيانات. يستلزم إخفاء البيانات وإخفاء هويتها إخفاء البيانات الحساسة عن طريق استبدال القيم الأصلية بقيم وهمية أو من خلال التحويلات التي تحافظ على بنية البيانات الأصلية. يعد هذا الأسلوب مفيدًا بشكل خاص عند مشاركة البيانات مع أطراف خارجية أو عندما تكون هناك حاجة إلى بيانات حساسة لأغراض التطوير أو الاختبار أو التحليل ولكن عندما لا تكون المعلومات الحساسة الفعلية مطلوبة. تدريب الموظفين وتوعيتهم تعتبر برامج التدريب والتوعية المنتظمة للموظفين ضرورية لحماية البيانات الحساسة. يجب أن يغطي التعليم أفضل ممارسات حماية البيانات، وكيفية الإبلاغ عن انتهاكات البيانات المحتملة أو نقاط الضعف. يعد خلق ثقافة الوعي الأمني أمرًا أساسيًا لتقليل المخاطر وحماية البيانات الحساسة من التهديدات الداخلية والخارجية. يجب أن يكون لدى كل مؤسسة خطة محددة جيدًا للاستجابة للحوادث، توضح بالتفصيل الخطوات التي يجب اتخاذها في حالة حدوث خرق للبيانات أو حادث أمني. يجب أن تتضمن هذه الخطة قنوات اتصال واضحة، والأدوار والمسؤوليات المعينة، وإجراءات ما بعد الحادث لتحليل الحدث والتعلم منه. تسمح خطة الاستجابة للحوادث التي يتم تنفيذها بشكل جيد للمؤسسات بالتخفيف من تأثير انتهاكات البيانات وحماية البيانات الحساسة بشكل فعال. الحماية القانونية من الإفصاح غير المصرح به توجد مخاوف تتعلق بخصوصية البيانات في جوانب مختلفة من الحياة اليومية حيثما يتم تخزين البيانات الشخصية وجمعها، ففي أكثر من 80 دولة حول العالم، تجري حماية معلومات التعريف الشخصية بموجب قوانين خصوصية المعلومات ، والتي تحدد للجهات العامة والخاصة مجال جمع واستخدام معلومات التعريف الشخصية. تتطلب مثل هذه القوانين عادةً من هذه الجهات تقديم إشعار واضح لا لبس فيه للفرد بشأن أنواع البيانات التي يتم جمعها، والاستخدامات المخططة للبيانات والمعلومات. وفي الأطر القانونية القائمة على الموافقة، تكون الموافقة الصريحة للفرد مطلوبة أيضًا. أصدر الاتحاد الأوروبي اللائحة العامة لحماية البيانات لتحل محل توجيه حماية البيانات السابق. فتم اعتماد اللائحة في 27 أبريل 2016. وأصبحت اللائحة قيد التنفيذ اعتبارًا ،(GDPR)

من 25 مايو 2018 بعد فترة انتقالية مدتها سنتان، فإنه لا يتطلب من الحكومات الوطنية تمرير أي تشريع تمكيني، وبالتالي فهو ملزم وقابل للتطبيق بشكل مباشر. "يعمل نظام حماية البيانات الجديد المقترح في الاتحاد الأوروبي على توسيع نطاق قانون حماية البيانات في الاتحاد الأوروبي ليشمل جميع الشركات الأجنبية التي تعالج بيانات المقيمين في الاتحاد الأوروبي. وهو ينص على تنسيق لوائح حماية البيانات في جميع أنحاء الاتحاد الأوروبي، مما يسهل الأمر على الشركات غير الأوروبية للامتثال لهذه اللوائح، فإن هذا يأتي على حساب نظام صارم للامتثال لحماية البيانات مع عقوبات صارمة تصل إلى 4٪ من حجم المبيعات في جميع أنحاء العالم . يوفر القانون العام لحماية البيانات أيضًا مجموعة جديدة من "الحقوق الرقمية" لمواطني الاتحاد الأوروبي في عصر تتزايد فيه القيمة الاقتصادية للبيانات الشخصية في الاقتصاد الرقمي. ينظم قانون حماية المعلومات الشخصية والوثائق الإلكترونية PIPEDA جمع واستخدام البيانات الشخصية والوثائق الإلكترونية من قبل المنظمات العامة والخاصة. يسري قانون (PIPEDA) في جميع الولايات القضائية الفيدرالية والإقليمية، باستثناء المقاطعات التي يتم فيها تحديد قوانين الخصوصية الحالية على أنها "متشابهة إلى حد كبير". نفذت الولايات المتحدة قدرًا كبيرًا من تشريعات الخصوصية المتعلقة بجوانب محددة مختلفة لخصوصية البيانات، مع التركيز على الخصوصية في الرعاية الصحية، وذلك على المستوى الفيدرالي وعلى مستوى العالم. على الرغم من أن هذه التشريعات لم تتم من خلال إطار المعلومات الحساسة الموحد. وسواء كانت القوانين منظمة أو ذاتية التنظيم، فإنها تتطلب إنشاء طرق يقتصر من خلالها الوصول إلى المعلومات الحساسة على الأشخاص ذوي الأدوار المختلفة، وبالتالي تتطلب في جوهرها إنشاء نموذج "مجال البيانات الحساسة" وآليات حمايته. تحتوي بعض النطاقات على إرشادات في شكل نماذج محددة قامت العديد من البلدان الأخرى بسن تشريعاتها الخاصة فيما يتعلق بحماية خصوصية ،HIPAA لـ "Safe Harbour" مسبقًا مثل البيانات، وما زال المزيد منها في طور القيام بذلك. يتم تحديد سرية المعلومات التجارية الحساسة من خلال اتفاقيات عدم الإفشاء، وهو عقد ملزم قانونًا بين طرفين في علاقة مهنية. قد تكون اتفاقيات عدم الإفشاء في اتجاه واحد، كما هو الحال في حالة حصول الموظف على معلومات سرية حول المنظمة التي يعمل بها، أو في اتجاهين بين الشركات التي تحتاج إلى مشاركة المعلومات مع بعضها البعض لتحقيق هدف تجاري مشترك. اعتمادًا على خطورة العواقب، قد يؤدي انتهاك عدم الإفشاء إلى فقدان الوظيفة، أو فقدان الاتصالات التجارية والعملاء، أو توجيه تهم جنائية أو دعوى مدنية، عندما يتم توقيع اتفاقيات عدم الإفشاء بين صاحب العمل والموظف عند بدء التوظيف، قد يكون شرط عدم المنافسة جزءًا من الاتفاقية كحماية إضافية لمعلومات العمل الحساسة، حيث يوافق الموظف على عدم العمل لدى المنافسين أو بدء أعمالهم التجارية المنافسة خلال فترة زمنية معينة أو حد جغرافي معين. على عكس المعلومات الشخصية والخاصة، لا يوجد إطار معترف به دوليًا لحماية الأسرار التجارية ، أو حتى تعريف متفق عليه لمصطلح "الأسرار التجارية" . فقد اتخذت العديد من البلدان والسلطات القضائية السياسية زمام المبادرة لمحاسبة انتهاك السرية التجارية في قوانينها الجنائية أو المدنية. بموجب قانون التجسس الاقتصادي الأمريكي لعام 1996، يعد اختلاس الأسرار التجارية مع العلم بأن ذلك سيفيد قوة أجنبية، أو سيلحق الأذى بمالك السر التجاري، أن انتهاك السرية التجارية يقع تحت القانون المدني، كما هو الحال في المملكة المتحدة. تكون قوانين الأسرار التجارية إما غير موجودة أو ضعيفة التطور ولا توفر إلا القليل من الحماية الجوهرية. يعد الكشف غير المصرح به عن معلومات مصنفة جريمة جنائية، وقد يعاقب عليها بالغرامات أو السجن أو حتى عقوبة الإعدام، اعتمادًا على خطورة الانتهاك. بالنسبة للانتهاكات الأقل خطورة، تتراوح من التوبيخ إلى إلغاء التصريح الأمني ثم إنهاء عقد العمل لاحقًا. الإبلاغ عن الفساد هو الكشف المتعمد عن معلومات حساسة لطرف ثالث بهدف الكشف عن أعمال مزعومة غير قانونية أو غير أخلاقية أو ضارة بأي شكل آخر. هناك أمثلة كثيرة لموظفين حكوميين حاليين وسابقين يكشفون عن معلومات سرية تتعلق بسوء سلوك الحكومة الوطنية للجمهور ووسائل الإعلام، على الرغم من العواقب الجنائية التي تنتظرهم.