إدارة البيانات المسؤولة:
مجموعة أدوات المدرب

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

المحتويات

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

عن مجموعة الأدوات

طورت هذه الوثيقة في إطار المشروع العالمي لأدلة مناهضة التعذيب (GATE)*، الذي تموله بسخاء وزارة الشؤون الخارجية الهولندية. وصممت مجموعة الأدوات هذه للاستخدام كمرجع من أجل عمل احترافي في مركز لإعادة تأهيل ضحايا التعذيب لتدريب الآخرين في مجال جمع البيانات المسؤولة. وهي توفر مقدمة لإدارة البيانات المسؤولة والأخلاقية وتمرينا عمليا عليها في سياق مناهضة التعذيب وحقوق الإنسان. ويمكن استخدامها كأداة مستقلة، أو بالاشتراك مع موارد أخرى عن إدارة البيانات المسؤولة.*

هذه الوثيقة من تأليف كاري جاستون.

1. مقدمة

المعلومات هي جزء جوهري لأي مؤسسة وأحد أصولها الأكثر قيمة. وحوكمة المعلومات وأساليب التعامل مع البيانات المسؤولة يوفران إطارا للتعامل مع هذه المعلومات. وعلى وجه التخصيص، التعامل مع المعلومات التي **تكشف عن هوية الشخص والسرية** بطريقة آمنة وسرية وحريصة.

يجب على كل شخص يعمل لدى مؤسسة أو بالنيابة عنها أن يكون على وعي بالآتي:

- أهمية المعلومات التي في حوزته التي ربما تكون سرية أو حساسة وترتبط بمستخدمي خدماتك أو الموظفين أو المتطوعين أو المانحين/الممولين أو أي شخص آخر له صلة بمؤسستك.
- التشريع المناسب في البلاد التي تعمل بها، وأيضا الإرشاد المناسب وأفضل الممارسات للبحث عن هذه المعلومات المهمة.
- لماذا يجب أن تكون مسؤولا عن كيفية حصولك على المعلومات وتسجيلها واستخدامها والاحتفاظ بها ومشاركتها.
- تأثير إدارة البيانات المسؤولة على استمرار العمل والقدرة على الاستمرار في توفير خدمة آمنة وموثوقة لمن تدعمهم.

إدارة البيانات المسؤولة مسؤولية كل شخص!

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

2. البيانات: تعريف الأنواع المختلفة للبيانات

في هذا القسم، ستعلم المشاركين في التدريب الأنواع والفئات المختلفة للبيانات، وكيفية التعرف عليها والأخطار والحماية المرتبطة بكل منها.

أهداف التعلم – بنهاية هذا القسم، سيكون المشاركون:

- *قادرين على التعرف على الفئات المختلفة للبيانات.*
- *فهم الأخطار المحتملة المرتبطة بالفئات المختلفة للبيانات.*
- *التفكير في كيفية تطبيق تدابير الحماية للأنواع المختلفة للبيانات في سياقاتهم.*
- *لديهم فهم لإخفاء هوية البيانات الشخصية.*

أنواع البيانات

في كل سياق مؤسسي، لكن بتحديد أكثر في أي نوع مؤسسة رعاية صحية أو اجتماعية، نحن نحتك بأنواع مختلفة من المعلومات الشخصية عن الناس.

من المهم أن نستطيع التعرف على هذه الأنواع المختلفة للمعلومات بحيث يمكن حمايتها كما ينبغي عند استخدامها ومشاركتها.

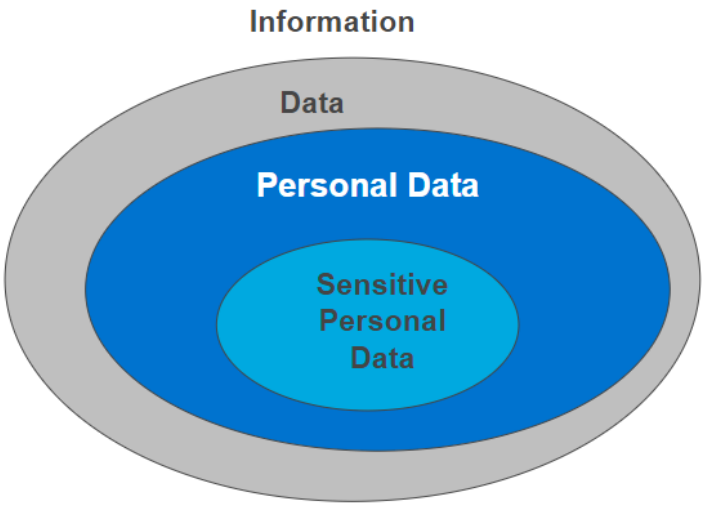
المعلومات هي أي مجموعة من الحقائق متوفرة أو معروفة عن شيء ما.

البيانات هي مجموعة من قيم المتغيرات النوعية أو الكمية.

البيانات الشخصية (pd) هي البيانات المرتبطة بشخص على قيد الحياة الذي يمكن التعرف عليه:

- من هذه البيانات،
- من هذه البيانات ومعلومات أخرى، التي تكون في حوزة الشخص أو المؤسسة ("مراقب البيانات" في علم مصطلحات حماية البيانات).

البيانات الشخصية الحساسة (spd) هي فئة خاصة للبيانات الشخصية التي ترتبط بالأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو المعتقدات المماثلة أو عضوية النقابة المهنية أو الحالة البدنية أو العقلية أو الحياة الجنسية أو ارتكاب أو ارتكاب مزعوم لأي جرم.



irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

المعلومات ***السرية*** هي المعلومات حيث تكون هناك حساسيات حول التعامل مع المعلومات وكشفها. وقد تكون طبيعتها إما شخصية أو مؤسسية. والبيانات الشخصية الحساسة عادة تعامل دائما على أنها سرية، وبالرغم من ذلك ليست جميع المعلومات السرية تكون طبيعتها حساسة أو شخصية. على سبيل المثال، معلومات العمل المؤثرة يمكن أن تندرج في هذه الفئة.

بالإضافة إلى التفكير في الكيفية التي تستطيع بها أنت ومؤسستك حماية البيانات من خرق من خارج مؤسستك، يجدر التفكير أيضا في كيفية تنفيذ ممارسة جيدة في التعامل السري مع البيانات ليس فقط خارجيا لكن أيضا داخل مؤسستك. وقد يعني ذلك أنه بجانب هذا التدريب، عليك أن تفكر في تنفيذ سياسات وإجراءات مؤسساتية تقدم لموظفيك إرشادا للممارسة الجيدة في التعامل مع أي شيء قد يعتبر معلومات سرية. وقد يعني ذلك تطوير سياسة السرية أو مدونة سلوك للموظفين.

اسأل المشاركين ما إذا كان باستطاعتهم التفكير في أي أنواع للمعلومات في سياقاتهم قد تندرج في هذه الفئة. واطلب من المشاركين كتابة هذه المعلومات في ورقة والتفكير في تدابير الحماية التي ربما تكون منفذة للتعرف على هذه الفئة للمعلومات وحمايتها. وبمجرد أن ينتهوا، ناقش الأمثلة التي كتبها المشاركون.

فيما يلي تمرين على تصنيف البيانات. اطلب من المشاركين تصنيف قائمة بمجموعات بيانات ممكنة في 3 فئات بتعريفهم كشخصية أو حساسة أو لا هذا ولا ذاك. والقائمة المقدمة نفسها تكون غامضة عمدا لكي يتشجع المشاركون لطرح أسئلة جديرة عن البيانات المقدمة بحيث يشعرون أنهم لديهم كافة المعلومات المطلوبة لتصنيف البند كشخصية أو حساسة. ويجب أن يثير التمرين مناقشة عن مجموعات البيانات الشخصية والحساسة، بحيث يقوي فهم المشاركين للتعريفات المختلفة.

كلما أمكن، كرر التمرين بنسخ فعلية حقيقية من مجموعات بيانات متنوعة التي تكون مستخدمة في سياقاتهم المحلية. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

-التفريق بين البيانات الشخصية والبيانات الشخصية الحساسة والبيانات التي لا هي شخصية ولا شخصية حساسة.

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

التمرين 1: فهم الأنواع المختلفة للبيانات

هذه بعض الأمثلة لمجموعات مختلفة من البيانات والمعلومات . اطلب من المشاركين وضعهم في الفئة المناسبة، حساسة أو شخصية أو لا هذا ولا ذاك . وأخبرهم أن يفكروا فيما إذا كان يجب التعامل مع البنود التي ليست شخصية ولا حساسة على أن طبيعتها "سرية" .

أيضا اطلب من المشاركين أن يفكروا فيما إذا كانوا قد يحتاجون إلى أي معلومات إضافية لتحديد الفئة المناسبة وأن يكتبوا أسئلتك .

بيانات شخصية حساسة	بيانات شخصية	بيانات (لا شخصية ولا شخصية حساسة)

تفاصيل بطاقات الائتمان لقائمة بالمانحين الجدد

قائمة تتضمن معلومات الصحة العقلية لمرضى العيادات

أسماء وعناوين العملاء

وثيقة تتضمن الـ 10 لغات الرئيسية لقاعدة عملائك وعدد المتحدثين بكل لغة

قائمة بالعملاء وانتماءاتهم السياسية، بدون استخدام أسماء ولكن أرقام تعريف

بيانات جغرافية مجمعة لكافة العملاء الذين حضروا إلى المركز في العام الماضي

قائمة بجميع العملاء البالغ عددهم 350 الذين حضروا العام الماضي، وانتماءهم العرقي وتوجههم الجنسي

نتائج استبيان بدون أسماء

قائمة بعناوين البريد الإلكتروني للعملاء الذين حضروا إحدى مجموعات يوم الجمعة

معلومات النتائج عن مجموعة من العملاء على سبيل المثال درجاتهم والتغيرات في الدرجات على مقياس للصحة العقلية قياسي

صور ضوئية لجوازات سفر أشخاص

معلومات عن مراكز الشرطة ومراكز الاعتقال المحددة بالاسم التي أخبرك العملاء عنها حيث تم احتجازهم بها

إحصائيات عن الـ 5 طرق تعذيب المختلفة الرئيسية والمعاملة اللا إنسانية التي أخبرك عنها قاعدة عملائك منذ افتتاح مركزك من 5 أعوام مضت

قائمة بجميع الأديان التي ينتمي إليها عملائك

تقرير داخلي يتضمن استخبارات حساسة عن العمل

لماذا تكون حماية المعلومات الشخصية مهمة؟ من المهم الامتثال للتشريع وأفضل ممارسة لحماية *المعلومات الشخصية*، لأن المعلومات الشخصية الحساسة تكون قيمة. والتعامل السيء مع المعلومات وحمايتها الضعيفة يمكن أن يسبب ضررا شخصيا واجتماعيا ويلحق الضرر بالسمعة. وفي سياقنا لإعادة تأهيل ضحايا التعذيب، قد يكون الخطر أكبر ويمس السلامة الشخصية للأفراد الذين يصلون إلى خدماتنا.

الطرق الشائعة لفقدان المعلومات:

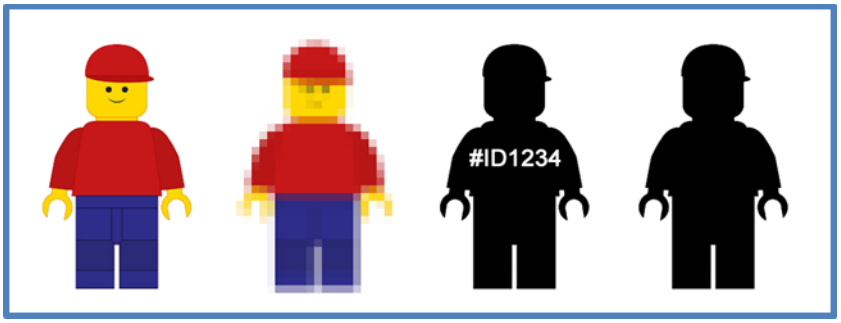
- فقدان المعلومات (بما في ذلك السجلات الورقية) عبر الهاتف أو عن طريق الفاكس أو فقدان أجهزة الحاسب أو الأجهزة النقالة.
- سرقة المعلومات بما في ذلك عن طريق هجمات التصيد الاحتيالي (انظر مسرد المصطلحات).
- التخزين والتخلص غير الآمن من المعلومات الذي يؤدي إلى فقدانها أو سرقتها.

الخطأ البشري يكون أكثر ضررا من الهجمات السيبرانية

من أكتوبر إلى ديسمبر 2017، كان الخطأ البشري مسؤولا تقريبا عن ثلثي الحوادث التي تم الإبلاغ عنها لمكتب مفوض المعلومات في بريطانيا (ICO) – الجهة المستقلة التي أنشئت لدعم حقوق المعلومات. وتسبب الخطأ البشري في فقدان أو ضرر أكثر من صفحات الويب غير الآمنة والقرصنة، التي تبلغ فقط 9% مجتمعة. وبالرغم من ذلك، يواصل جذب السوق لانتباه العملاء وموارده التركيز على التهديدات الخارجية، تحديدا الهجمات السيبرانية والقراصنة.

- يكشف تصنيف لمكتب مفوض المعلومات (ICO) لأنواع الخروقات بسبب الخطأ البشري عن الأسباب الرئيسية كالآتي:
  - البيانات المرسلة بالبريد الإلكتروني إلى المستلم الخطأ (15.8%).
  - فقدان وسرقة العمل الورقي (13.1%).
  - البيانات المرسلة بالبريد أو بالفاكس إلى المستلم الخطأ (13.0%).
- أسباب أخرى شملت التخلص غير الآمن من الأجهزة والعمل الورقي، وفقدان أو سرقة أجهزة غير مشفرة، وعدم الالتزام بتنقيح البيانات.

إزالة "الشخصية" من "البيانات الشخصية": إخفاء هوية البيانات وإخفاء الهوية باستخدام بيانات مستعارة



إخفاء هوية البيانات باستخدام بيانات مستعارة هو إجراء تستبدل به الحقول الأكثر تعريفا في سجل بيانات بمعرف واحد أو أكثر اصطناعي أو بأسماء مستعارة. ويمكن أن يكون هناك اسم مستعار واحد لمجموعة من الحقول المستبدلة أو اسم مستعار لكل حقل مستبدل. ويساعد ذلك في إخفاء الهوية الحقيقية لشخص ***لكن*** ليس إخفاء حقيقيا للهوية لأن الهوية يمكن بسهولة اكتشافها لأنها الأساس للتشفير المستخدم.

الاسم: أليشا سانتوس تاريخ الميلاد: 21 إبريل 1980 التعليم: بكالوريوس علم نفس، جامعة جويلف مكان الميلاد: شلالات نياجرا، أونتاريو - كندا الوظيفة الحالية: أستاذ رياضيات في جامعة كمبريدج الحالة الاجتماعية: متزوجة من دين أودونيل عدد الأطفال: 3	إخفاء هوية البيانات باستخدام بيانات مستعارة	رقم الهوية 357986 تاريخ الميلاد: 21-4-1980 التعليم (أعلى مستوى): 4 مكان الميلاد: شلالات نياجرا، أونتاريو - كندا الوظيفة الحالية: أستاذ جامعي الحالة الاجتماعية: متزوجة أطفال: نعم

إخفاء هوية البيانات هي عملية تحويل البيانات إلى شكل لا يُعرّف هوية الأشخاص حيث من غير المرجح أن يحدث التعرف على هويتهم. ويسمح ذلك باستخدام أوسع نطاقا للمعلومات.

"نحن نستخدم مصطلح "بيانات مجهولة الهوية" للإشارة إلى البيانات التي لا تكشف هي نفسها عن أي شخص، والتي من غير المرجح أن تسمح بالتعرف على أي شخص من خلال دمجها مع بيانات أخرى". (مدونة قواعد ممارسة إخفاء البيانات لمكتب مفوض المعلومات، صفحة 6)

الاسم: أليشا سانتوس تاريخ الميلاد: 21 إبريل 1980 التعليم: بكالوريوس علم نفس، جامعة جويلف مكان الميلاد: شلالات نياجرا، أونتاريو - كندا الوظيفة الحالية: أستاذ رياضيات في جامعة كمبريدج الحالة الاجتماعية: متزوجة من دين أودونيل عدد الأطفال: 3	إخفاء هوية البيانات	رقم الهوية: 357986 الفئة العمرية: 30-40 التعليم (أعلى مستوى): شهادة جامعية مكان الميلاد: جنوب أونتاريو - كندا الوظيفة الحالية: مدرس الحالة الاجتماعية: متزوجة أطفال: نعم

كلمة سريعة عن التجميع....

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

تجميع البيانات هي أي عملية يتم بها جمع المعلومات وإظهارها في شكل موجز، لأغراض مثل التحليل الإحصائي. وطالما أن بياناتك لا ***تعرف شخصا*** ، فإنها لم تعد تخضع لنفس أوجه الحماية التشريعية نفسها، على الرغم من استمرار كونها حساسة للعمل تماما، ولذلك تظل في حاجة إلى حماية (انظر أيضا *المعلومات السرية* أعلاه).

سيساعد التمرين الآتي المشاركين في التفكير في كيفية ارتباط بياناتهم في سياقاتهم بفئات البيانات التي تناولها النقاش أعلاه. وسيساعد الجزء (ب) المشاركين في التفكير في الكيفية التي يمكنهم بها حماية فئات معينة من البيانات، على سبيل المثال باستخدام أساليب إخفاء هوية البيانات. وبنهاية التديب يجب أن يكون المشاركون قادرين على:

- سرد مجموعات البيانات في سياقهم.

- تعريف مجموعات البيانات هذه كبيانات شخصية أم لا.

- إجراء مناقشة عن ما هي البيانات التي قد تكون بحوزة مؤسستهم التي ليست بيانات شخصية لكن ربما تظل تحتاج إلى التعامل معها على أنها سرية.

- البدء في التفكير في تنفيذ تدابير حماية للأنواع المختلفة من البيانات.

- التفكير في كيفية تطبيق إخفاء هوية البيانات على البيانات الشخصية قبل مشاركتها.

- ربما البدء في التفكير في ترتيبات مشاركة البيانات.

التمرين 2: فهم الأنواع المختلفة للبيانات في سياقك

(أ) اسرد مجموعات البيانات الشائعة التي تعالجها (الجمع، التعامل مع، الإبلاغ، التخزين، إلخ) وجربها وصنفها في الفئات المختلفة التي تناولها النقاش أعلاه (بيانات شخصية (pd)، بيانات شخصية حساسة (spd)، لا هذا ولا ذاك). وهل أي من مجموعات البيانات هذه من المحتمل أن تكون "سرية"، لكن لا تندرج في الفئة "شخصية"؟ هل المخاطر المرتبطة بهذه البيانات تكون مختلفة؟ هل ستطبق نفس تدابير الحماية على هذا النوع من البيانات؟

(ب) فكر في مجموعة بيانات تعمل بها (على سبيل المثال، قائمة عملاء) التي قد تتطلب مشاركتها. هل يمكنك التفكير في الكيفية التي يمكنك بها حماية هذه المعلومات قدر المستطاع قبل مشاركتها؟

3. حماية البيانات في التشريع (الاتحاد الأوروبي)

في هذا القسم، ستقدم الإطار التشريعي لحماية البيانات. ويطبق هذا التشريع المحدث مؤخرا فقط في الاتحاد الأوروبي لكن من المفيد التعرف عليه باعتباره عيار الذهب في حماية البيانات بعدد من الطرق. كما أنه مفيد كأداة لتعلم ممارسة جيدة، حتى إذا لم يكن التشريع يطبق مباشرة في منطقتك المحددة من العالم.

أهداف التعلم – بنهاية هذا القسم، سيكون المشاركون:

- *لديهم فهم للتشريع الحالي الذي يحكم حماية البيانات في الاتحاد الأوروبي*

- *لديهم فهم للحقوق الفردية لمواضيع البيانات ومسؤوليات مراقبي ومعالجي البيانات*
- *التفكير في كيفية تطبيق تدابير حماية الأنواع المختلفة للبيانات في سياقاتهم*
- *التفكير في كيفية إكمال تمرين تعيين البيانات لتحديد نوعية البيانات المحتفظ بها وأين*
- *فهم ماذا يكون طلب وصول موضوع وكيفية الامتثال لطلب، بما في ذلك التنقيحات*

الإطار التشريعي الأوروبي: مقدمة للقانون العام لحماية البيانات (GDPR)

القانون العام لحماية البيانات (GDPR) هو تشريع جديد يقدم قانونا واحدا لخصوصية البيانات للاتحاد الأوروبي. وهو يرتكز على تشريع حماية البيانات الحالي ويقويه في المجالات الرئيسية الآتية:

التعريفات:

- "موضوع البيانات" هو أي شخص تعالج مؤسستك بياناته الشخصية.
- "مراقب البيانات" هي الجهة التي تحدد أغراض وأحوال ووسائل معالجة البيانات الشخصية.
- "معالج البيانات" هي الجهة التي تعالج البيانات بالنيابة عن مراقب البيانات.

⬅ ***حقوق الأشخاص*** – بموجب GDPR، تكون حقوق موضوع البيانات مدعمة أو محسنة في عدد من المجالات. وتشمل هذه المجالات،

- **الحق في الاطلاع** – مواضيع البيانات لديهم الحق في معرفة من يفعل ماذا ببياناتهم.
- **حق الوصول** – مواضيع البيانات لديهم الحق في الوصول إلى البيانات الشخصية التي تحتفظ بها عنهم – يشمل ذلك تقديم نسخة من بياناتهم لهم وأن يكون ذلك مجانا وخلال إطار زمني معقول (انظر أيضا أدناه طلبات وصول المواضيع).
- **الحق في التصحيح** – مواضيع البيانات يمكنهم طلب إجراء تغييرات على البيانات التي تحتفظ بها عنهم حيثما تعتبر زائفة أو قديمة أو ناقصة.
- **الحق في المحو** – مواضيع البيانات الآن لديهم الحق في طلب محو معلوماتهم – يعرف ذلك أيضا "بالحق في النسيان".
- **الحق في تقييد المعالجة** – مواضيع البيانات يمكنهم طلب منع أو وقف معالجة بياناتهم الشخصية. وفي هذه الظروف، قد يتطلب الأمر أن يستمر معالجو البيانات في تخزين بيانات مرتبطة بموضوع البيانات لدعم ذلك. (مثال لذلك يمكن أن يكون حيثما طلب مانح أو داعم مؤسسة ما بعدم الاتصال به مجددا لطلب دعم مالي. وعندئذ ستكون البيانات المحتفظ بها هي القيمة الدنيا لدعم طلب عدم الاتصال به مجددا).
- **الحق في قابلية نقل البيانات** – السماح لمواضيع البيانات بالحصول على ونقل وإعادة استخدام البيانات عبر الخدمات أو لأغراضهم الخاصة.
- **الحق في الاعتراض** – مواضيع البيانات لديهم الحق في الاعتراض على معالجة بياناتهم بما في ذلك للتسويق أو لإنشاء ملفات التعريف.
- **الحقوق المرتبطة باتخاذ القرار المؤتمت، بما في ذلك إنشاء ملفات التعريف** – هناك متطلبات محددة لكي تكون ممتثلا للتشريع فيما يخص اتخاذ القرار المؤتمت.

➡ GDPR أيضا يقوي أو يحسن ***مساءلة مراقبي البيانات***، حيث يتوقع منهم تطبيق إجراءات حوكمة شاملة، وتشجيع المساءلة والشفافية.

⬅ يشمل ذلك أيضا التزامات أوسع نطاقا بشأن ضمان ***امتثال المعالجين***، بما في ذلك المقاولين.

- كما يشمل ***التزامات بخصوص الإبلاغ عن خروقات البيانات***، ووجود شخص مسؤول (مسؤول حماية بيانات) في المؤسسات الكبرى، والجهات العامة والجهات التي تقوم بمعالجة واسعة النطاق للبيانات الشخصية.
- حماية البيانات بواسطة التصميم/افتراضيا – التفكير في تنفيذ إجراءات لحماية البيانات في تصميم أي نظام جديد قبل حدوث جمع البيانات.
- تقييمات تأثيرات الخصوصية – منح الاهتمام المستحق لأي تأثيرات محتملة على خصوصية الأفراد لجميع أنشطة المعالجة.

كلمة عن طلبات وصول المواضيع....

بموجب تشريع حماية البيانات الحالي والمقترح فإن أي موضوع بيانات له الحق في طلب أي بيانات شخصية عنه تحتفظ بها أي مؤسسة. ويعني ذلك أن أي شخص يمكنه طلب نسخة أو عرض المعلومات التي يحتفظ بها معالج بيانات أو مراقب بيانات عنه، ولا يمكن رفض الامتثال للطلب. وعند الامتثال لأي من هذه الطلبات، من المهم الحفاظ على مبادئ (الحقوق الفردية) مواضيع البيانات – التي ربما تنقح بعض المعلومات حيثما تكون هذه المعلومات قد تم جمعها من مصادر أطراف ثالثة لكن تشكل جزء من السجل الذي تحتفظ به.

اطلب من المشاركين التفكير في الكيفية التي سيمتثلون بها لطلب وصول موضوع من شخص يستخدم خدماتهم. ما الذي قد يحتاجون إليه للامتثال لأي من هذه الطلبات؟ اطلب منهم التفكير في أمثلة حيث يوجد سجل ربما يتضمن معلومات تتطلب تنقيح قبل الامتثال لطلب؟ ناقش هذه الأشياء كمجموعة.

تعيين البيانات

لحماية البيانات كما ينبغي، والامتثال للنقاط أعلاه، فإنك تحتاج أولا إلى معرفة نوعية البيانات التي تحتفظ بها، وأين. وتكون فكرة جيدة أن تكمل تمرين تعيين بيانات، بحيث أنك والآخرين في مؤسستك تكونون على بينة بنوعية البيانات المحتفظ بها، ومكان تخزينها، وكم مضى على الاحتفاظ بها، ومتى وكيف يتم إتلافها.

أشياء للتفكير فيها....

ما البيانات الشخصية التي لديك؟ للإجابة عن هذا السؤال، ستحتاج إلى إجراء مراجعة كاملة وتدقيق لكافة البيانات الشخصية التي تجمعها، على سبيل المثال:

- هل لديك معلومات مكتوبة في قصاصات ورق في درج في مكتبك؟
- هل لديك معلومات شخصية مكتوبة في مفكرة ورقية؟
- هل تستطيع الامتثال لطلب وصول موضوع (SAR)؟

أين تخزنها؟

- في قاعدة بيانات؟
- على أجهزة مشتركة/أجهزة شبكة؟ من لديه وصول إليها؟
- في مفكرات ورقية؟ في قصاصات ورقية في مكتبك؟
- في المنزل؟ في رسائل بريد إلكتروني؟

أين ترسلها؟

- هل تستطيع تأكيد أنك ترسل معلومات العميل داخل بلدك فقط؟
- هل لديك إذن صريح كتابي/موثق لإرسال البيانات؟ هل تستطيع إثبات ذلك؟

كيف تعالجها؟

- على أجهزة حاسبات؟
- قطع من الورق؟
- كيف تحمي أي بيانات عند نقلها؟

ماذا تخبر الناس/مواضيع البيانات عن المعالجة؟

- هل لديك معلومات متاحة بحرية لمواضيع البيانات؟
- عرف معالجي الأطراف الثالثة؟
- هل تعبر البيانات أي حدود وطنية/دولية؟

توكيد المعلومات العلاجية: هل هي المعلومات الصحيحة؟ دقيقة؟ هل تدققها وتحدثها بانتظام؟ هل هناك دليل يثبت ذلك؟

سيساعد التمرين الآتي المشاركين في التفكير كليا في نوعية البيانات التي يجمعونها ويحتفظون بها، وكيف وأين يتم تخزينها. وسيساعدهم ذلك في معرفة ليس فقط نوعية البيانات التي ربما يحتاجون إلى حمايتها، لكن أيضا نوع تدابير الحماية التي ربما يحتاجون إلى تنفيذها للأنواع المختلفة للبيانات. كما سيلقي الضوء على أين يمكن أن تكون هناك ثغرات في الإدارة المناسبة للبيانات. وبنهاية التديب يجب أن يكون المشاركون:

- لديهم فهم لمواقع والأشكال المختلفة التي تتخذها بياناتهم.

- التفكير في مكان وكيفية تخزينها، ومن لديه وصول إليها.

- التفكير في مدى أهمية النقاط أعلاه في الحق في المحو أو في الاستجابة لطلب وصول موضوع.

- البدء في التفكير في الجداول الزمنية للاحتفاظ بالبيانات.

التمرين 3: تعيين البيانات

اختر مجموعة بيانات مناسبة لمركزك (على سبيل المثال معلومات عملاء) وأكمل تمرين تعيين البيانات الآتي بالإجابة عن الأسئلة الآتية:

- *ما البيانات التي تم جمعها؟*
- *هل تم الحصول على موافقة عند نقطة الجمع؟*
- *أين تم تخزين المعلومات؟ في قاعدة بيانات أم ملف ورقي أم ملف حاسب؟*
- *فيما تستخدم البيانات؟*
- *من يمكنه الوصول إليها؟*
- *هل جرى مشاركتها خارجيا في أي وقت؟*
- *كيف/متى تم مراجعة/الإضافة إلى/تحديث البيانات؟*
- *كم مضى على الاحتفاظ بها؟*
- *متى تم حذفها وكيف؟*

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

التعلم من الآخرين: خروقات البيانات في الأنباء...

المؤسسة الخيرية لمرضى الزهايمر وجد أن بها عيوب خطيرة في الطريقة التي تعاملت بها مع بيانات شخصية حساسة، بما في ذلك اكتشاف متطوعين كانوا يستخدمون عناوين البريد الإلكتروني الشخصية لتلقي ومشاركة معلومات عن الناس الذي يستخدمون المؤسسة الخيرية، وتخزين بيانات غير مشفرة على حواسبهم المنزلية وعدم الالتزام بالاحتفاظ بالسجلات الورقية في مكان مأمون. (ICO، 7-1-2016)

عيادة صحية تم تغريمها 180 ألف جنيه استرليني (204,000 يورو، 253,000 دولار أمريكي) لخرق البيانات عندما أرسلت بغير عمد رسالة إخبارية بها عناوين البريد الإلكتروني لمستلمي الرسالة في حقل "إلى"، بدلا من حقل "نسخة مخفية"، وبذلك إفشاء حالة مرض نقص المناعة البشرية "الإيدز" لمستلمي الرسائل فعليا. (ICO، 9-5-2016)

العثور على ذاكرة USB في غرب لندن تحتوي على بيانات أمن المطار (Register، 30-10-2017)

التفاصيل الشخصية لطفل متبني وللوالدين والاختصاصيين الاجتماعيين أرسلت بغير عمد إلى مدعوين إلى حفلة (Chronical Live، 26-12-2017).

خزانة حفظ ملفات لأوراق حكومية سرية ينتهي بها المطاف في متجر للأغراض المستعملة. (Guardian، 2-2-2018)

ما يجب وما لا يجب في السرية

يجب

- حماية سرية كافة معلومات تعريف الأشخاص أو المعلومات السرية التي تحتك بها.
- إدراك أن أي معلومات مسجلة عن شخص ما يجب حمايتها – يشمل ذلك الملاحظات والمفكرات.
- ترتيب مكتبك في نهاية كل يوم، وحفظ كافة السجلات المنقولة التي تتضمن معلومات تعريف أشخاص أو معلومات سرية في أماكن حفظ ملفات أو تخزين متعارف عليها تكون مقفلة في الأوقات التي لا يكون الوصول إليها مراقب أو تحت إشراف مباشرة.
- إيقاف تشغيل الحاسبات التي بها وصول إلى معلومات تعريف أشخاص أو معلومات عمل سرية، أو جعلها محمية بكلمة مرور، إذا تركت مكتبك لأي فترة من الوقت.
- الحرص على عدم سماع الآخرين لك عندما تناقش أمورا سرية.
- الاستعلام والتحقق حسب الضرورة من هوية أي شخص يطلب معلومات تعريف أشخاص أو معلومات سرية والتأكد من أنهم بحاجة إلى معرفتها.
- مشاركة فقط الحد الأدنى من المعلومات الضرورية.
- الحرص عند إرسال فاكس أو رسالة بريد إلكتروني وحيثما أمكن الاحتفاظ بإيصال بالاستلام/بالقراءة
- نقل معلومات تعريف الأشخاص أو المعلومات السرية بطريقة آمنة على سبيل المثال باستخدام تشفير البريد الإلكتروني.
- طلب النصيحة إذا كنت تحتاج إلى مشاركة معلومات تعريف شخص بدون موافقة الشخص الذي يمكن التعرف عليه وسجل القرار وأي إجراء تم اتخاذه.
- الإبلاغ عن أي خروقات للسرية فعلية أو محل شك.
- المشاركة في جلسات التعريف والتدريب ورفع الوعي بمسائل السرية.

لا يجب

- **لا** تشارك كلمات المرور أو تتركها مباحة للآخرين لكي يرونها.
- **لا** تشارك المعلومات بدون موافقة الشخص الذي تخصه المعلومات، إلا إذا كانت هناك أسباب قانونية لعمل ذلك
- **لا** تستخدم معلومات تعريف الأشخاص إلا إذا كانت ضرورية لا محالة؛ اخف هوية المعلومات حيثما أمكن.

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

- **لا** تجمع أو تحتفظ بمعلومات أو تعالج معلومات أكثر مما تحتاج إليه ولا تحتفظ بها أطول من اللازم.
- **لا** تظن أن التعليقات أو الملاحظات التي تسجلها تراها أنت فقط؛ الأشخاص لديهم الحق في الوصول إلى المعلومات المحفوظة عنهم بتقديم طلب وصول موضوع.
- **لا** تترك المعلومات بدون رقابة على مكتبك.
- لا تترك **أبدا** ملفات أو معلومات في السيارة أو الحافلة أو عند العمل من المنزل، وتأكد من أن المعلومات لا يمكن أن يصل إليها أي شخص غيرك.

سيساعد التمرين الآتي المشاركين في التفكير جيدا في الممارسات الحالية في مؤسستهم باستخدام بعض معضلات حماية البيانات الشائعة. ويجب أن يحفزهم على التفكير في كافة الطرق التي يتعاملون ويخزنون وينقلون بها المعلومات الحساسة هم وزملائهم. ويجب أن يفكروا في ممارسات العمل المختلفة والخطر على البيانات الذي ربما تنطوي عليه هذه الطرق. ويجب أن يفكروا في تدابير الحماية الممكنة لتقليل الخطر على البيانات. وقد ترغب في أن تطلب من المشاركين أن يفكروا هم أنفسهم في بعض السيناريوهات، ترتبط مباشرة بمؤسستهم أو تجربتهم. وبنهاية التديب يجب أن يكون المشاركون:

- قادرين على تحديد الأخطار المحتملة المصاحبة لممارساتهم المؤسسية.

- قادرين على تحديد تدابير الحماية لتقليل الأخطار التي حددوها أعلاه.

التمرين 4: أشياء للتفكير فيها

فكر فيما قد تفعله في حالة السيناريوهات الآتية:

1. *أنت في عجلة من أمرك لتغادر المركز. أنت تريد ملاحظاتك ووثائقك لتبدأ MLR (تقرير طبي شرعي) الذي تخطط أن تفعله على حاسبك المحمول أثناء رحلة القطار الطويلة إلى المنزل.*

   فكر في: ما الأخطار المحتملة لحماية البيانات؟

   كيف يمكنك تقليلها؟

2. *أنت تعمل في المنزل في إحدى الأمسيات على مسودة MLR الذي تريد مراجعته في اليوم التالي. كيف يمكنك تقليل الأخطار على حماية البيانات؟*

3. *أنت تعثر على بعض النسخ الورقية بها مواد حساسة للعميل في المنزل. كيف ستتعامل مع هذا الأمر؟*

4. *أنت تدرك أنك بدون عمد أرسلت بالبريد الإلكتروني بعض معلومات العميل إلى عنوان البريد الإلكتروني المنزلي لزميل لك. ما الذي ستفعله؟ من الذي ستخبره بهذا الخطأ؟*

سيساعد التمرين الآتي المشاركين في فهم كيفية الامتثال لطلب وصول موضوع بموجب الإطار التشريعي لحماية البيانات الموجز أعلاه. سيحتاج المشاركون إلى الرجوع إلى تمرين تعيين البيانات السابق (التمرين 3) للعثور على كافة المعلومات التي قد تكون لديهم عن شخص ما، سواء في شكل نسخة ورقية أو إلكترونية. كما يجب أن يفكروا في أي من المعلومات التي احتفظوا بها تتضمن معلومات أطراف ثالثة، والكيفية التي يمكن أن ينقحوا بها هذه المعلومات استجابة لطلب وصول موضوع (SAR). كما يجب عليهم التفكير في العواقب المحتملة للشخص والتأكد من أنهم يفهمون ذلك جيدا قدر المستطاع (على سبيل المثال إرسال بيانات صحية حساسة عن طريق بريد إلكتروني غير آمن، إلخ). وبنهاية التمرين يجب أن يعرف المشاركون:

- الخطوات التي عليهم اتخاذها للتعامل مع طلب وصول موضوع.

التمرين 5: الامتثال لطلب وصول موضوع

أنت تستلم رسالة بريد إلكتروني من شخص ما يدعي أنه المحامي لعميل بالمركز، وأنه يطلب نسخة من السجلات التي تحتفظ بها عنه كطلب وصول إلى موضوع. كيف ستمتثل للطلب؟ ما الذي تحتاج إلى أخذه في الاعتبار للامتثال على النحو الصحيح وفي وقته؟

التمرين الآتي يكون لجعل المشاركين يفكرون فيما يشكل خرقا لحماية البيانات أو خرقا للسرية ولمحاولة ورؤية الأهمية التي يقدرونها لخطورة هذه الخروقات. وفي تقديرهم للأهمية، يجب أن يقدموا لك تفسيرا لكيفية لتحديد أن حادثة كانت أكثر أهمية أو خطورة من غيرها. كما يجب عليك أن تجعلهم يفكرون في سياقهم وإضافة حوادثهم إلى القائمة. وعندما تحدث خروقات، كيف سيضمنون أنهم يتعلمون منها ولا تتكرر؟ وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- تحديد ما الذي يشكل خرقا للبيانات.

- تحديد النطاقات المختلفة لخطورة الخروقات المختلفة للبيانات

التمرين 6: رتب السيناريوهات الآتية حسب خطورتها، من الأكثر إلى الأقل

- *أنت تعثر على نسخ لوثائق متروكة في آلة ناسخة في المكتب – تشمل الوثائق خطابات وقائمة بمخاوف صحة عقلية وبدنية لشخص ما.*
- *زميل يخبرك أنه أرسل بالبريد الإلكتروني معلومات عميل تتضمن بيانات صحية حساسة شخصية إلى عنوان البريد الإلكتروني الخطأ.*
- *زميل يخبرك أنه كان مسافرا وبصحبته بيانات عميل وأنه تركها غير متعمد بالحافلة/القطار/مكان ما لا يستطيع أن يتذكره.*
- *عميل قلق جدا يأتي إليك ويخبرك بأن معلوماته ومعلومات عدد من العملاء الآخرين وجدت على الإنترنت. وأن هذه المعلومات تتضمن بيانات صحية حساسة.*
- *أنت تكتشف أن مكتبك تم اقتحامه في الليل. إحدى خزانات حفظ الملفات التي تتضمن معلومات عملاء قد فتحت بأسلوب الكسر والملفات مفقودة.*
- *أنت تكتشف أن زميلا أرسل بالبريد الإلكتروني تقريرا طبيا كاملا لعميل إلى عدد من الأشخاص الخارجيين لكي يستخدموه كتمرين تدريب، بدون الموافقة الكتابية للعميل.*
- *إداري أرسل بدون عمد معلومات عملاء (أسماء، خصائص سكانية) إلى شركة محاماة حيث أرسلت الأوراق بالبريد مع تقرير طبي شرعي بعد اكتماله.*
- *تقرير طبي شرعي يتضمن بيانات شخصية حساسة بدرجة كبيرة تم توزيعه لمندوبي تدريب بدون إخفاء مناسب لهوية البيانات.*
- *إداري قدم معلومات عن عميل عبر الهاتف بدون اتباع للضوابط الضرورية فيما يتعلق بما إذا كان الشخص لديه موافقة للمعلومات.*

إدارة البيانات المسؤولة: الصورة الأكبر إلى ما بعد مجرد حماية البيانات

حتى الآن، أنت ناقشت حماية البيانات، وأنواع البيانات التي تكون مناسبة بموجب أطر تشريعية معينة. وفي هذا القسم فإنك ستتقدم إدارة البيانات المسؤولة للمشاركين – التي تغطي مجموعة أكبر من الأفكار والسلوكيات والاعتبارات التي تنطبق على دورة حياة البيانات الكاملة، وليس فقط السياق المحدد لمجموعات بيانات تعريف الأشخاص.

أهداف التعلم – بنهاية هذا القسم، فإن المشاركين:

- *سيتعرفوا على مفهوم "البيانات المسؤولة".*
- *سيطوروا فهما للتأثيرات الأوسع نطاقا للبيانات المسؤولة والأخلاقية في الإدارة الكلية للبيانات.*
- *سيكتشفوا العواقب الممكنة لعدم ممارسة إدارة البيانات المسؤولة.*

ما البيانات المسؤولة؟

الواجب الجماعي لتفسير العواقب غير المتعمدة للعمل بالبيانات بواسطة:

1) إعطاء الأولوية لحقوق الناس في القبول والخصوصية والحماية والملكية عند استخدام البيانات في جهود التغيير الاجتماعي ودعمه،

2) تطبيق قيم وممارسات الشفافية والصراحة.

ما إدارة البيانات المسؤولة؟

إدارة البيانات المسؤولة هي عن التعامل مع البيانات التي نجمعها باحترام والحفاظ على حقوق الناس الذين نجمع بياناتهم.

هي أن تكون مسؤولا ومنتبها للتأثيرات على الناس في جميع جوانب إدارة البيانات شاملا **الجمع** و**التعامل مع** و**التخزين** و**الاستخدام**.

هي أن تكون مسؤولا عن بيانات الناس الآخرين من نقطة الجمع إلى نشر التقرير.

اعتبارات البيانات المسؤولة

تشمل العناصر الأساسية لممارسة البيانات المسؤولة:

ديناميكا النفوذ: تكون الأطراف الأقل نفوذا في أي موقف غالبا أول من يرى العواقب غير المتعمدة للبيانات المجمعة عنهم. والعمليات مثل التصميم المشترك أو ضمان اشتراك ناس من خلفيات متنوعة في جمع البيانات أو عمليات التحليل يمكن أن تقلل تأثير ذلك.

على سبيل المثال، في الأزمات الإنسانية، يكون الناس الذين تجمع منهم البيانات أقل نفوذا من الذين يطلبون منهم بياناتهم. كيف يمكن لهذا اللاتماثل في النفوذ أن يؤثر على رغبتهم في إعطائهم بياناتهم لاستخدامها؟

التنوع والانحياز: الأخذ في الاعتبار أسئلة مثل، "من يتخذ القرار؟ ما الجوانب المفقودة؟ كيف يمكننا أن نضمن تنوعا للفكر والأسلوب؟" يمكن أن ينير البقع المعتمة، والمجالات حيثما يكون إضافة أصوات إضافية له قيمته.

نحن نؤمن بأن التنوع بكافة أنواعه يقوي مشروعاتنا وأسلوبنا. وقد شهدنا مشروعات ومنتجات ومؤسسات تعاني من موظفين أو مجتمعات متماثلين – وغالبا، يكون أول من يرى ويتحمل التأثيرات السلبية للبيانات هم المجتمعات المهمشة. ونحن نحتاج إلى تضمين هذه الأصوات وتوفير طرق للتحسين كنتيجة.

المجهولات غير المعروفة: نحن لا نستطيع أن نرى المستقبل، لكن يمكننا أن نضع موانع وموازين لتنبيهنا إذا كان شيء ما غير متوقع يحدث.

غالبا، "لكننا لم نكن نعرف" هو أول شيء نسمعه عندما تكون هناك عواقب سلبية غير مقصودة لمشروع مرتبط بالبيانات. ومسؤوليتنا أن نفكر في الكيفية التي نستطيع بها إنشاء وكلاء للعواقب المهمة أو غير المتعمدة شديدة التأثير تحديدا.

مبدأ الاحتياط: مجرد أننا نستطيع استخدام البيانات بطريقة معينة، لا يعني بالضرورة أننا يجب أن نستخدمها. وإذا كنا لا نستطيع تقييم الخطر وفهم الأضرار على نحو كاف عند التعامل مع البيانات، عندئذ ربما يجب علينا التوقف لدقيقة وإعادة تقييم ما نفعله وسببه.

تقدم لنا التقنية جميع أنواع الإمكانيات. وليست جميعها ذكية، ولن يكون لجميع الإمكانيات تأثيرات جيدة على العالم. وإذا كنا نعمل في مجال التغيير الاجتماعي، فإن أولويتنا هي احترام وحماية حقوق الناس – ويتطلب ذلك منا أن نكون عميقي الفكر في تصرفاتنا.

الابتكار عميق الفكر: لكي تحظى الأفكار الجديدة بأفضل فرصة ممكنة للنجاح – ولكي يستفيد كل شخص من هذه الأفكار والمشروعات الجديدة – يحتاج الابتكار إلى التوصل إليه بحرص وبفكر، ليس فقط السرعة.

الابتكار هو عن العثور على حلول أفضل وأكثر فعالية لتلبية أفضل للاحتياجات. ولعمل ذلك، يجب علينا أولا أخذ الوقت الذي نحتاج إليه للتفكير في تلك الاحتياجات – ربما من خلال البحث وربما بطرق أخرى. بعد ذلك يجب أن نفكر في الحلول الممكنة التي يمكن أن تلبي تلك الاحتياجات، وبشكل حاسم، سيكون لها تأثيرات إيجابية (بدون تأثيرات جانبية سلبية غير مقصودة) على الناس الذين نحاول دعمهم على المدى الطويل.

التمسك بمعايير أعلى: في حالات كثيرة، لم تدرك الأطر القانونية والتشريعية بعد التأثيرات الحقيقية للبيانات والتقنية. كيف يمكننا أن نجتهد ليكون لدينا معايير أعلى وأن نكون نموذجا يحتذى به؟

العمل في التغيير الاجتماعي ودعمه يعني أننا نجتهد لخلق مجموعة معينة من النماذج. الربح ليس هدفنا – التغيير الاجتماعي الإيجابي هو هدفنا. في مناطق كثيرة من العالم، الأطر التنظيمية لها ثغرات تسمح للمشروعات التي، إذا فكرنا فيها مرة أخرى، ربما تعتبر استغلالية. والبلاد المختلفة لديها معايير مختلفة لأوجه الحماية القانونية للخصوصية – مثل القانون العام لحماية البيانات القادم الذي يحمي الحقوق بقوة.

بناء سلوكيات أفضل: لا يوجد أسلوب واحد يصلح لجميع ظروف البيانات المسؤولة. فالثقافة والسياق والسلوكيات القائمة تغير التأثيرات والطرق التي تستخدم بها البيانات.

البيانات المسؤولة ليست ممارسة مكتسبة بالتقادم – للأسف لا توجد أي قوائم تدقيق لاجتيازها ثم اعتبارها "مسؤولة". ومعظم ذلك يكون عن بناء أساليب مدروسة أفضل للعمل بالبيانات – التي ربما تتضمن مراجعة القرارات التي نتخذها بانتظام، بسبب المعلومات الجديدة. وممارسة البيانات المسؤولة ليست مجرد مهمة للأشخاص الذين يتعاملون مع البيانات مباشرة – إنها مسألة عملياتية يحتاج كل شخص، من القيادة إلى الموظفين، إلى التفكير فيها.

إذا كان الأمر يخصك أنت، ويخص بياناتك، كيف ترغب في التعامل معها/احترامها/الحفاظ عليها آمنة؟

السرية – يجب أن يكون الوصول إلى البيانات مقصورا على الأشخاص الذين لديهم سلطة مناسبة.

التكامل – يجب أن تكون البيانات كاملة ودقيقة. يجب أن تعمل جميع الأنظمة والأصول كما هو متوقع.

الإتاحية – يجب أن تكون المعلومات متاحة وتسلم إلى الشخص المناسب، في الوقت المناسب، عند الحاجة إليها.

اطلب من المشاركين التفكير في السيناريو الآتي، الذي يلقي الضوء على مسائل عن تكامل البيانات والسرية. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- تحديد تلك المسائل عن تكامل البيانات والسرية.

- توقع العواقب الممكنة التي ربما تحدث للعميل.

التمرين 7: تكامل البيانات والسرية

السيناريو

JP هو عميل للمركز ويحضر مواعيد منتظمة لعلاج نفسي مرتبط بتعذيب تعرض له عندما أعتقلته شرطة الولاية.

نتيجة لخطأ مُدخل بيانات، يتصل إداري بطريق الخطأ برقم هاتف عمله بدلا من رقم هاتفه الشخصي ونظرا لوجود JPفي اجتماع، يرفع أحد زملائه السماعة. ومع اعتقاد الإداري أن JP هو من رد على الهاتف، فإنه يواصل ليسأله ما إذا كان باستطاعته تغيير موعده لوقت لاحق.

مع كشف الإداري عن المكان الذي تأتي منه المكالمة، يتضح فورا لزميل JP أنه يتلقى علاجا من المركز، ويواصل كشف هذه المعلومات أكثر إلى زملاء آخرين.

الأسئلة:

- *ما الدروس التي يمكن تعلمها من السيناريو أعلاه؟*
- *ما العواقب المحتملة لـ JP؟*

تلميحات:

- *رقم هاتف العمل يكون حيثما يجب أن يكون رقم الهاتف الشخصي.*
- *السرية تخترق عندما يخبر الإداري شخص ما آخر غير JPمعلوماته الشخصية.*

4. دورة حياة البيانات

في هذا القسم، سوف تقدم دورة حياة البيانات للمشاركين وتجعلهم يفكرون في اعتبارات البيانات المسؤولة المناسبة لكل خطوة. وسوف تطلب من المشاركين اجتياز بعض التمرينات العملية لممارسة أساليب إدارة البيانات المسؤولة. ويجب أن يفكر المشاركون في الأنواع المختلفة للأخطار والتهديدات التي يجب أخذها في الاعتبار في المراحل المختلفة لدورة حياة إدارة البيانات.

أهداف التعلم – بنهاية هذا القسم، سيكون المشاركون:

- *يفهمون دورة حياة البيانات، وكيف تناسب اعتبارات إدارة البيانات المسؤولة كل خطوة.*
- *يفهمون كيفية تقييم الخطر عندما يتعلق بإدارة البيانات وإكمال تقييم أخطار يضع في الاعتبار تدابير الحماية الممكنة.*
- *يفهمون كيفية الاهتمام بخصوصية الناس عند التفكير في إدارة البيانات وما هو تقييم تأثير الخصوصية.*

فهم دورة حياة بياناتك

دورة حياة البيانات هي تسلسل للمراحل التي تجتازها وحدة معينة للبيانات بداية من إنشائها الأولي أو الاستحواذ عليها إلى أرشفتها النهائية أو حذفها. وهناك غالبا 6 مراحل أو أكثر محددة في دورة حياة البيانات العادية، تغطي **جمع**، **التعامل مع**، **تخزين** و**استخدام** البيانات.

I. الجمع

1. التخطيط – حاول التفكير في النتائج التي تحاول تحقيقها وأنواع المعلومات التي ستحتاج إلى جمعها لكي تحرز النجاح.
2. تقييم الأخطار – هل تطرح السؤال لأنه سيحسن مجموعة بياناتك، أم هناك سبب آخر؟
3. تدريب الفريق وجامعي البيانات الآخرين – التأكد من أن الفريق يفهم ويطبق أساليب التعامل مع البيانات المسؤولة.
4. الموافقة – تعتبر عيار ذهب للممارسة الجيدة لضمان موافقة مدروسة سليمة عند الحصول على البيانات الشخصية واستخدامها.

II. التعامل مع وIII. التخزين

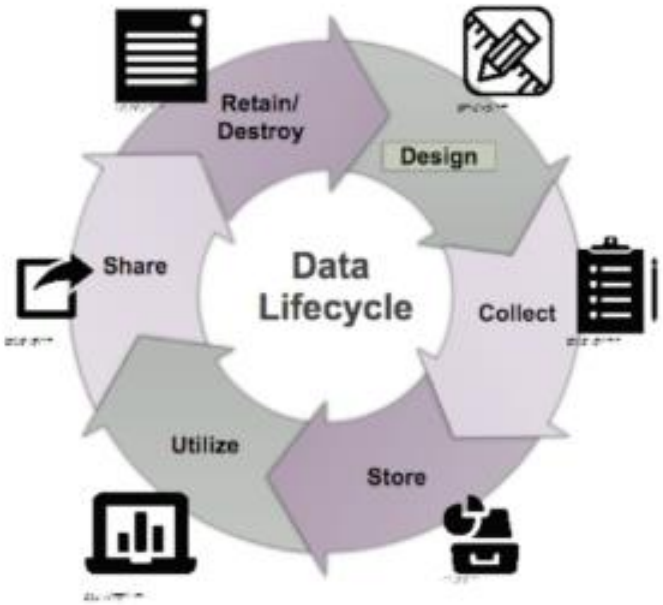
5. الإدارة – كيف ستجمع وتخزن وتستخدم وتشارك؟ كيف ستضمن أن بياناتك تكون دقيقة؟ هل تحتاج إلى تنفيذ تدابير لمراجعة وتنقية وإزالة البيانات بانتظام؟

IV. الاستخدام

6. الاستخدام – كيف ستستخدم ما تم جمعه؟
7. الملاحظات – أمر أساسي للإدارة الأخلاقية للبيانات هو التأكد من أن الأشخاص الذين اطمئنوا إلى تقديم بياناتهم الشخصية لك يحصلون على ملاحظات كلما أمكن عن الأشياء الجيدة التي تم تحقيقها باستخدام بياناتهم.

التعامل مع البيانات وتخزينها

8. الاحتفاظ والإتلاف – ما المدة التي أحتاج إلى الاحتفاظ ببياناتي خلالها؟ هل أحتاج إلى الاحتفاظ بكافة البيانات، أم فقط بعضها؟ هل يمكنني إخفاء هوية البيانات؟



I. الجمع

التخطيط: تقييمات الأخطار، تقييمات تأثيرات الخصوصية، الموافقة المدروسة، التدريب.

الخطوة 1: ضع **خطة**. حدد بوضوح غرض جمع البيانات. يجب أن تتناسب الفوائد التي تتوقعها من جمع البيانات مع الأخطار. يجب أن توجهك مصالح ورفاهية الأشخاص الذين تجمع البيانات عنهم. لا تجمع بيانات أكثر من الضرورية. خطط إخفاء هوية البيانات بواسطة التصميم كلما أمكن. خطط الكيفية التي ستحصل بها على موافقة مدروسة قبل أن تبدأ. راجع طرق جمعك للبيانات بحثا عن أي انحياز بها. كيف ستتحقق من دقة ونقية بياناتك؟

الخطوة 2: قم بإجراء **تقييم أخطار**. جمع البيانات يمكن أن يضع الناس في خطر. قيم الأخطار واتخذ إجراء لتجنب العواقب السلبية، على سبيل المثال بالتأكد من حماية وسرية البيانات.

خطر الخصوصية هو خطر الضرر الذي ينجم من خلال اقتحام الخصوصية. وبعض الطرق التي يمكن أن ينشأ بها الخطر تكون من خلال أن المعلومات الشخصية تكون:

- غير دقيقة أو غير كافية أو قديمة؛
- زائدة عن الحد أو غير مناسبة؛
- تم الاحتفاظ بها لمدة طويلة جدا؛

- تم كشفها للأشخاص الذين لا يريد الشخص الذي تكون عنه البيانات في حصولهم عليها؛
- استخدمت بطرق لا يقبلها أو يتوقعها الشخص الذي تكون عنه؛ أو
- لم يتم حفظها بطريقة آمنة.

يمكن للضرر أن يتمثل بطرق مختلفة. وأحيانا سيكون ملموسا ويمكن قياسه كميا، على سبيل المثال خسارة مالية أو فقدان وظيفة. وفي أوقات أخرى سيكون أقل تحديدا، على سبيل المثال ضرر بالعلاقات الشخصية والوضع الاجتماعي ناجم عن الكشف عن معلومات سرية أو حساسة.

يحاول تقييم تأثير للخصوصية تقييم والإبلاغ عن التأثيرات المحتملة على خصوصية الشخص عندما تعالج المؤسسات البيانات الشخصية.

أشياء تؤخذ في الاعتبار عند إجراء تقييمات تأثيرات الخصوصية:

- ما سبب جمع معلومات تعريف الشخص؟
- هل الأشخاص الذين أجمع بيانات عنهم أبدوا اختيارا وموافقة على المعالجة؟
- هل لدي سياسات تحكم استخدام ومعالجة معلومات تعريف الأشخاص؟ هل هذه السياسات قوية وتناسب الغرض؟
- هل يتلقى الموظفون دعما وتدريبا منتظما؟
- هل هناك إزالة لسجلات التدقيق لمكان تخزين ونقل بياناتك؟
- هل هناك إزالة لبروتوكولات مشاركة المعلومات منفذة؟

سيساعد التمرين الآتي المشاركين في التفكير في جميع جوانب إدارة البيانات قبل البدء في مشروع أو خدمة جديدة. يجب على المشاركين أن يختاروا بوضوح مشروعا أو عملية جديدة ويفكروا في جميع جوانب إدارة البيانات المسؤولة (RDM) في خطتهم. ويجب أن يلقي هذا التمرين الضوء على أهمية التفكير في RDM قبل بدء أي مشروع أو عملية أو خدمة جديدة، بحيث يمكن دمج مبادئ RDM ومشاركتها من البداية.

يجب على المشاركين البدء في التفكير في نهاية دورة البيانات من البداية – والتفكير في نوع الأسئلة التي يحاولون الإجابة عنها من البداية – على سبيل المثال، نص حر مقابل بيانات مصنفة، ومزايا وعيوب كل منها. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- تحديد ممارسات RDM عبر دورة حياة البيانات من البداية إلى النهاية.

التمرين 8: ضع خطة

اطلب من المشاركين أن يقسموا أنفسهم إلى ثنائيات أو مجموعات صغيرة، ويبتكروا خطة لمشروع أو خدمة جديدة ستقدمها مؤسستهم. وتأكد من تناولهم الآتي في خططهم:

- ما الذي يحاول المشروع أو الخدمة تحقيقه؟
- ما الغرض من جمع البيانات، وماذا ستفعل بها؟
- ما الطرق التي ستستخدمها لجمع البيانات؟
- كيف ستحصل على موافقة مدروسة؟
- كيف ستدرب فريقك؟
- ما الأخطار وكيف ستتعامل معها؟

- ما الشكل الذي ستكون عليه البيانات؟ مصنفة، غير مصنفة، نص حر؟
- ما الشكل الذي تحتاج البيانات إلى أن تكون عليه، لكي توافق نوع التحليل الذي ترغب في عمله، إن وجد؟ هل يحتاج إلى أن يتوافق مع مجموعات بيانات أخرى؟ (على سبيل المثال اتفاق فئات أم تجمعات)
- كيف ستتعامل مع استجابات البيانات المصنفة حيثما لا يكون هناك وجود لهذه الاستجابات (على سبيل المثال شخص تكون إجابته "لا هذا ولا ذاك" عن السؤال "ما نوعك؟" والإجابات في نظامك هي "ذكر، أنثى")
- ما تدابير الحماية التي تحتاج إلى استخدامها بخصوص الوصول، ونقل، وتخزين، ومشاركة البيانات؟
- كم المدة التي خلالها ستحتفظ/تؤرشف/تتخلص من البيانات؟ هل لديك أي طريقة لإخفاء هوية البيانات قبل أرشفتها؟

سيساعد التمرين الآتي المشاركين في التفكير عمليا في جميع الأخطار المصاحبة للأنواع المختلفة للتعامل مع البيانات وتنفيذ تدابير حماية للتعامل مع هذه الأخطار. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- تقدير وموازنة خطر جمع البيانات لصالح استخدام هذه البيانات.

التمرين 9: تقييم أخطار التعامل مع البيانات

.اطلب من المشاركين إكمال الجدول أدناه، وتقييم الأخطار وتحديد درجة خطر لكل واحد من الأخطار واطلب منهم إكمال الضوابط الحالية لديهم التي ربما تكون موضع تنفيذ وتجربة وتحديد ضوابط إضافية ربما يحتاجون إلى استخدامها .وقد تم إدراج بعض الاقتراحات الممكنة في الجدول لهم .أضف أخطار إضافية للتقييم عندما يحددونها.

تحديد الخطر والتأثير (التأثيرات) المحتملة	نوع الخطر	درجة الخطر قبل السيطرة: احتمال x خطر (حد أدنى صفر وحد أقصى 25)	الضوابط الحالية/الضمانات	درجة الخطر بعد السيطرة احتمال x خطر	إجراءات مخططة إضافية
وصول/عرض غير مسموح به فقدان وثائق ورقية أثناء نقلها					
احتفاظ موظفين/متطوعين بوثائق في المنزل/خارج مكان العمل					
رسائل بريد إلكتروني ترسل من عناوين بريد إلكتروني شخصية					
وثائق أرسلت إلى المستلم الخطأ					
فقدان أو سرقة حاسبات محمولة أو ذاكرات USB					
بيانات غير دقيقة أو ناقصة					
بيانات مكررة					

الخطوة 3: **درب** فريق عملك. تأكد من أن فريق عملك يعرفون ويفهمون اعتبارات حماية البيانات والبيانات المسؤولة. وتأكد من أنهم يجرون تقييمات أخطار. وتأكد من أنهم يعرفون كيفية الحصول على موافقة مدروسة. وتأكد من أنهم يتدربون على أفضل ممارسة لأمان البيانات.

الخطوة 4: احصل على **موافقة مدروسة**. أخبر المستجيبين عن الكيفية التي ستستخدم بها بياناتهم وسبب احتياجك إليها.

- **اشرح**. اشرح للناس بوضوح كيف ستستخدم معلوماتهم الشخصية ودلهم على معلومات إضافية عن ذلك – على سبيل المثال، على موقع ويب مؤسستك أو في منشور أو ملصق إعلاني.
- **امنح اختيارا**. امنح الناس اختيارا عن كيفية استخدام معلوماتهم وأخبرهم ما إذا كان هذا الاختيار سيؤثر على الخدمات المقدمة إليهم.
- **حقق التوقعات**. استخدم المعلومات الشخصية فقط بالطرق التي سيتقبلها الناس على نحو معقول.

في هذا التمرين، سيفكر المشاركون في الكيفية التي يمكنهم بها الحصول على موافقة مدروسة في سياقهم. ويجب أن يفكروا في كافة الطرق التي يستخدمون بها بيانات العميل، وأن يحرصوا على ذكرها في أي نموذج موافقة. ويجب أن يفكر المشاركون في الحصول على موافقة من الناس المعرضين للخطر الذين ربما يحتاجون إلى شرح الأمور لهم بعدة طرق مختلفة، والذين ربما لا يفهمون تماما ما هي الموافقة، والذين قد يسحبون فيما بعد الموافقة التي سبق أن منحوها. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- التأكد من أن نماذج الموافقة تعكس الطرق التي تستخدم بها مؤسستهم (وتعتزم بها استخدام) معلومات العملاء.

- الأخذ في الاعتبار مسائل الموافقة المرتبطة بالناس المعرضين للخطر.

التمرين 10: الموافقة المدروسة

أ) مع وضع خدماتك وسياقك في الاعتبار، طور نموذج موافقة يغطي الاستخدامات المختلفة للبيانات في مؤسستك. وتأكد من أن يكون نموذجك واضحا وموجزا ويعكس بدقة حيثما يكون هناك اختيار لمنحه.

وربما ترغب أيضا في ضمان أن نموذجك يغطي ترتيبات مشاركة البيانات العامة حيثما يمكن أن تشارك خدمتك البيانات مع آخرين بانتظام (على سبيل المثال خدمات صحة أخرى، إلخ).

ب) مع شريك/في ثنائيات، تمرن على اجتياز نموذج الموافقة والحصول على موافقة مدروسة.

II. التعامل مع البيانات وتخزينها

الخطوة 5: **أدر بياناتك**

التأكد من جودة البيانات: نق، احم، حسن.

فكر فيما ستحتاج إلى تنفيذه لضمان أن تكون سجلاتك وبياناتك متكاملة: منقاة ولا يوجد بها بيانات مكررة ولا يوجد بها أخطاء.

أشياء للتفكير فيها عن:

ما العواقب المحتملة للبيانات غير المنقحة؟ فكر تحديدا في إدارة يوم بيوم لخدمة ما (انظر المثال أعلاه بخصوص: JP) وأيضا في أي نوع تحليل أو اتخاذ قرار الذي ربما يأتي من بيانات المشارك. ما نوع المعلومات أو الاستنتاجات، أو تصور الآخرين عن هذه البيانات؟ ما السياسات أو العمليات التي ربما يحتاجون إلى استخدامها لضمان بيانات بنوعية جيدة؟

في التمرين الآتي، سيفكر المشاركون في قيمة البيانات المنقحة والقياسية، والأخطار المحتملة من البيانات سيئة الجودة. وسيتعلمون تقييس مجموعة صغيرة وكيفية إسهام ذلك في بيانات منقاة وربما يقلل الأخطاء في التحليل. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- تنقية البيانات.

- فهم كيفية إسهام تنقية/تقييس البيانات في تكامل البيانات.

التمرين 11: تنقية/تقييس البيانات

اطلب من المشاركين إلقاء نظرة على مجموعة البيانات الآتية واقتراح طرق لتنقيتها أو تقييسها.

جان دو	نيويورك	علاج سريري	1978-1-15
أحمد أسان	ن.ي.	علاج	15 يناير 1978
جورجو قنسطنطين	ني	سريري	1978/1/15

- النقل – كن حريصا عند استخدام أجهزة نقالة أو عند نقل سجلات ورقية. شفر السجلات الرقمية. قيد الوصول. تأكد من تشفير الأجهزة. كن أكثر حرصا عند نقل سجلات ورقية التي تكون عرضة لخطر فقدانها أو سرقتها.
- الوصول – تأكد من أن الوصول يكون مقيدا على أساس "الحاجة إلى المعرفة". قيد الوصول إلى الأنظمة والسجلات. تأكد من أن السجلات الورقية تكون في مكان مأمون طوال الوقت والوصول إليها مراقب.
- التخزين – تأكد من أنك تعرف وتفهم أين تكون معلوماتك مخزنة، و
- المشاركة – هل ستحتاج إلى مشاركة جميع أو جزء من بياناتك؟ على سبيل المثال، سجلات فردية تدعم عميل، أو، مجموعات بيانات أكبر مع شريك بحث؟

سيتعلم المشاركون كيفية إعداد اتفاقية رئيسية لمشاركة البيانات، تضع في الاعتبار مسائل حماية البيانات والقيمة الممكنة لمشاركة البيانات. ويجب أن يفكر المشاركون فيما إذا كانت وسائل إخفاء هوية البيانات تكون مناسبة في سياق المثال الذي اختاروه. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- فهم مسائل حماية البيانات عند مشاركة البيانات.

- إنشاء اتفاقية بسيطة لمشاركة البيانات.

التمرين 12: اتفاقية مشاركة البيانات

اطلب من المشاركين التفكير في الشركاء الذين يعملون معهم وحيثما قد يحتاجون إلى مشاركة البيانات. طور اتفاقية صورية لمشاركة البيانات لهذا الغرض.

تهدف السيناريوهات الآتية إلى حمل المشاركين على التفكير في كيفية موازنتهم لاحتياجات الخدمة مع مبادئ حماية البيانات. وبنهاية التمرين يجب أن يكون المشاركون قادرين على:

- موازنة أي مصالح متعارضة عند التفكير في إدارة البيانات المسؤولة.

التدريب 13: أشياء للتفكير فيها عن

كيف ستستجيب أو تنصح زملائك استجابة للسيناريوهات الآتية:

- *أنت تسجل بيانات قبول طلب من ناج ويسأل ماذا سيحدث للمعلومات التي يقدمها لك.*
- *أنت تأخذ معلومات تاريخ السوابق من ناج عن طريق مترجم، وبالرغم من أن الناجي قدم إجابة طويلة جدا ومؤثرة عن سؤال، قدم المترجم بوضوح ملخصا لما قاله.*
- *مؤسسة شريكة تريد عمل مشروع تعاوني مما يعني مشاركة البيانات. ما الذي يمكن أن تحتاج إلى التفكير فيه/تنفيذه عند التفكير في ذلك؟*
- *زميل جديد ينضم إلى مؤسستك ويسأل عن سياستك بخصوص العملاء الذين يوافقون أو يرفضون الموافقة على استخدام بياناتهم لأنشطة معينة. ماذا تقول له؟*

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

III. الاستخدام

الخطوة 6: **استخدم** بياناتك! قد يكون ذلك ممارسة ضغط أو دعم أو تعلم ينطبق على خدماتك. فكر فيمن يكون ممثلا في البيانات. هل فكرت في أي انحياز؟ موازنة النوع؟ هل أنت واثق في جودة بياناتك؟ في جودة التحليل؟

الخطوة 7: قدم **ملاحظات**. تكون ممارسة جيدة أن تشرك الأشخاص الذين تجمع منهم بيانات في استخدامها. على سبيل المثال، إذا كنت استخدمت بياناتك في كتابة تقرير لأغراض الدعم، فإنها تكون ممارسة جيدة أن تشارك هذا التقرير مع المستجيبين حيثما يمكن.

الخطوة 8: **الاحتفاظ والإتلاف**. تأكد من أن لديك سياسات مناسبة للاحتفاظ بالبيانات وإتلافها منفذة. هل تحتاج إلى الاحتفاظ بالبيانات بشكلها الحالي؟ هل أنت مضطر إلى الاحتفاظ ببيانات شخصية؟ هل توجد طريقة للاحتفاظ فقط ببيانات مجمعة؟ أو إخفاء هويتها؟ إذ كان لا، هل تستطيع استرداد سجلات الأشخاص لإتلافها (انظر "الحق في المحو" أعلاه تحت GDPR). عند اختيار الحذف، التأكد من أن الحذف يكون نهائيا ومن حذف جميع النسخ/الإصدارات أيضا.

تمتد إدارة البيانات المسؤولة والفعالة طوال دورة الحياة الكاملة للبيانات.

الخاتمة: من أين نبدأ؟ أشياء يمكنك أن تبدأ في عملها الآن

- ارفع الوعي بين زملائك والمقاولين والشركاء بخصوص التعامل الآمن مع البيانات – خصيصا مع أقدم الأشخاص في مؤسستك.
- درب فريق عملك وتواصل معهم بخصوص إدارة البيانات المسؤولة وإجراءات أمان البيانات، بما في ذلك سياسات ضمان منع الوصول إلى البيانات عندما يغادر الموظفون المؤسسة.
- تأكد من أن لديك سياسات وإجراءات قوية للتعامل الآمن مع البيانات الشخصية وحمايتها. السياسات: حماية البيانات، أمن البيانات، السرية، مشاركة البيانات، الإبلاغ عن الحوادث (الخرق)، الاسترداد، الإفشاء.
- تأكد من وجود خطوط واضحة للمساءلة عندما يتعلق الأمر بالتعامل مع البيانات.
- تأكد من وجود شفافية في التعامل مع البيانات وتأكد من أن الأشخاص الذين تتعامل مع بياناتهم الشخصية يفهمون بوضوح الكيفية التي سيتم بها استخدام بياناتهم.
- نفذ تقييم أخطار وتقييمات تأثيرات الخصوصية كلما تفكر في جمع نماذج جديدة للبيانات أو جمع بيانات بطريقة مختلفة. ووجود خطة سيساعدك في التفكير في الأخطار والعواقب المحتملة في حالة حدوث خرق للبيانات.
- استخدم أسلوب يراعي الأخطار وفكر فيما يمكن أن يفشل لكي تجرب وتجهز تدابير وقائية لتقليل الخطر.
- واجب المسؤول: كن جاهزا لتكشف عن حالات الخروقات أو فقدان غير متعمد للبيانات أو فساد البيانات عند حدوثها.
- تاكد من أنك لديك عقود قوية جاهزة لتغطية المسائل بخصوص مشاركة البيانات أو حيثما تسند معالجة البيانات إلى مقاول من الباطن.
- راجع أمن تقنية المعلومات، وتأكد من وجود تدابير مناسبة للتشفير، والنسخ الاحتياطي للبيانات والتحديثات وBYOD (أحضر جهازك الخاص) وهي سياسة السماح للموظفين بإحضار أجهزتهم الخاصة إلى العمل، إلخ.
- تأكد من أنك لديك خطة استجابة للحوادث في حالة خرق البيانات.

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

5. مسرد المصطلحات

التجميع – شكل للتجميع في فئة أو مجموعة لأغراض التحليل أو إخفاء هوية البيانات على مستوى أعلى.

خرق البيانات – حادثة أمان تتعرض فيها **البيانات** الحساسة أو المحمية أو السرية إلى النسخ أو النقل أو العرض أو السرقة أو استخدامها بواسطة أشخاص غير مصرح لهم بعمل ذلك.

توافق البيانات – اكتمال مجموعة بيانات.

تنقية البيانات – عملية اكتشاف وتصحيح (أو إزالة) سجلات فاسدة أو غير دقيقة من مجموعة سجلات أو جدول أو قاعدة بيانات وتشير إلى تحديد أجزاء ناقصة أو غير صحيحة أو غير دقيقة أو غير مناسبة من البيانات ثم استبدال أو تعديل أو حذف البيانات غير الصالحة أو الرديئة.

مراقب البيانات – شخص/مؤسسة الذي يحدد الأغراض والأسلوب الذي تعالج به أو سوف تعالج به أي بيانات شخصية.

حوكمة البيانات – عملية (عمليات) محددة لمؤسسة لضمان بقاء البيانات عالية الجودة طوال دورة حياتها.

صحة البيانات – العمليات الجماعية التي يتم إجراؤها لضمان نقاء *البيانات*. تعتبر البيانات نقية إذا كانت خالية من الأخطاء نسبيا. والبيانات غير الصالحة يمكن أن يتسبب فيها عدد من العوامل تشمل السجلات المكررة أو البيانات الناقصة أو القديمة، والتحليل غير السليم لحقول السجلات من أنظمة متفاوتة.

دورة حياة البيانات – تدفق المعلومات خلال نظام، بداية من الإنشاء والتخزين إلى الحذف.

معالج البيانات – أي شخص/مؤسسة تعالج البيانات الشخصية بالنيابة عن مراقب البيانات.

مسؤول حماية البيانات – الشخص (الأشخاص) المسؤول عن التأكد من أن المؤسسة (المؤسسات) تمتثل لتشريع حماية البيانات، وغالبا للسياسات الداخلية لحماية البيانات.

مجموعة البيانات – مجموعة من البيانات المرتبطة ببعضها.

اتفاقية مشاركة البيانات – اتفاقية أو إطار لمشاركة البيانات يوضح كيفية نقل وتخزين واستخدام البيانات.

تقييس البيانات – العملية الحرجة لوضع البيانات في تنسيق عام يسمح بالبحث التعاوني والتحليلات واسعة النطاق ومشاركة الأدوات والمنهجيات المتطورة.

موضوع البيانات – شخص يكون هو موضوع البيانات الشخصية.

التشفير – عملية ترميز الرسائل والمعلومات بطريقة لا يستطيع أن يقرأها إلا الأطراف المصرح لهم. ولا يمنع التشفير في حد ذاته اعتراض الرسائل لكن يرفض استقبال محتوى الرسالة المرسلة إلى المعترض.

GDPR – القانون العام لحماية البيانات – التشريع الجديد الذي يحكم حماية بيانات موضوع البيانات في الاتحاد الأوروبي.

مفوض المعلومات – السلطة المسؤولة عن مراقبة وفرض تشريع حماية البيانات في المملكة المتحدة.

أخلاقيات المعلومات –"فرع الأخلاقيات الذي يركز على العلاقة بين إنشاء وتنظيم ونشر واستخدام المعلومات، والمعايير الأخلاقية ومدونات الأخلاق التي تحكم أداء الإنسان في المجتمع".

حوكمة المعلومات – إدارة المعلومات في مؤسسة. توازن حوكمة المعلومات استخدام وأمان المعلومات.

الموافقة المدروسة – موافقة تمنح طواعية وبحرية، على أساس تقدير وفهم واضحين لحقيقة وتأثيرات والعواقب المحتملة مستقبلا لعمل ما.

البيانات الشخصية – البيانات المرتبطة بشخص على قيد الحياة الذي يمكن التعرف عليه من البيانات، أو من تلك البيانات ومعلومات أخرى التي تكون في حوزة، أو من المرجح أن تصبح في حوزة، مراقب البيانات.

التصيد الاحتيالي – محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقات الائتمان (وأحيانا بشكل غير مباشر، أموال) غالبا لأسباب شريرة، بالتنكر ككيان جدير بالثقة في اتصال إلكتروني.

المعالجة – جمع أو تعديل أو التعامل مع أو تخزين أو كشف معلومات شخصية.

تقييم تأثير الخصوصية – تقييم يجرى للتحقق من تأثير أي معالجة جديدة على خصوصية مواضيع البيانات. أداة لتحديد أخطار الخصوصية وتقليلها.

الاسم المستعار – اسم وهمي أو منتحل.

إدارة السجلات – مجال الإدارة المسؤولة عن المراقبة الفعالة والنظامية لإنشاء واستلام وصيانة واستخدام وترتيب السجلات. ويشمل ذلك تحديد وتصنيف وتخزين وحماية واسترداد وتتبع وإتلاف أو الاحتفاظ بالسجلات بصفة دائمة.

التنقيح – مراقبة أو إخفاء جزء من نص أو معلومات لأغراض قانونية أو أمنية أو الخصوصية أو إخفاء الهوية.

البيانات الشخصية الحساسة – تشير إلى بيانات عن:

- الأصل العرقي أو الإثني.
- الانتماءات السياسية.
- الدين أو المعتقدات المماثلة.
- عضوية النقابة المهنية.
- الصحة البدنية أو العقلية.
- الصفة الجنسية.
- السجل الجنائي أو الدعاوى القضائية.

طلب وصول موضوع (SAR) – أي طلب (كتابي) بواسطة موضوع بيانات من أجل معلومات شخصية عنه تكون في حوزة مؤسسة.

6. المراجع/الموارد الإضافية

لجنة جودة الرعاية. *بيانات آمنة، رعاية آمنة.* https://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf

مفوض حماية البيانات في أيرلندا *GDPR and you* http://gdprandyou.ie/

DLA Piper، *قوانين العالم لحماية البيانات.* https://www.dlapiperdataprotection.com/index.html?t=world-map&c=DK

القانون العام لحماية البيانات https://www.eugdpr.org/

Geraghty, R. (2016). *إخفاء هوية البيانات والبحث الاجتماعي.* https://www.slideshare.net/ISSDA/anonymisation-and-social-research?qid=fa5a5338-8766-4b0b-9bf6-105f852d5932&v=&b=&from_search=1

مكتب مفوض المعلومات https://ico.org.uk/

مكتب مفوض المعلومات (2017). *الاستعداد للقانون العام لحماية البيانات (GDPR): 12 خطوة لتتخذها الآن.* https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

مكتب مفوض المعلومات (2017). مدونة *أخلاقيات ممارسة وصول الموضوع: التعامل مع الطلبات من الأشخاص من أجل المعلومات الشخصية.* https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

مكتب مفوض المعلومات. *أحضر جهازك الخاص (BYOD).* https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

ICRC. *المعايير المهنية لعمل الحماية.* https://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf

حارس البيانات الوطنية للصحة والرعاية. *مراجعة أمان البيانات، والموافقة والخيارات.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

NHS Digital. *الوعي بأمان البيانات المستوى 1* https://www.igt.hscic.gov.uk/

NHS England. *كتيب حوكمة المعلومات.*

منتدى البيانات المسؤولة: https://responsibledata.io/

مصلحة البيانات البريطانية. *إخفاء هوية البيانات.* https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation

الملحق أ

قالب برنامج التدريب

أهداف التدريب: تطوير المهارات والمعرفة بخصوص إدارة البيانات المسؤولة (الجمع والتعامل مع والتخزين والاستخدام)، وتطوير المهارات لتدريب الآخرين.

اليوم الأول

0900-10:30 (1.5 ساعة)

مقدمة لإدارة البيانات المسؤولة

- لماذا تحتاج إلى حماية؟
- فكر في الكيفية التي تريد بها معاملة بياناتك الخاصة

أي بيانات؟

- البيانات الشخصة، البيانات الحساسة

← تمرين: تحديد وتصنيف البيانات الشخصية/الحساسة/السرية

- إخفاء هوية البيانات وإخفاء الهوية باستخدام بيانات مستعارة
- التجميع

← تمرين: سرد مجموعات البيانات المعالجة عادة في سياقك؛ تصنيف مجموعات بياناتك؛ البدء في التفكير في مشاركة البيانات

10:30: راحة (15 دقيقة)

10:45-12:30 (1.75 ساعة)

مقدمة GDPR الأوروبي / الإطار التشريعي

- GDPR: الإطار القانوني للاتحاد الأوروبي. السياق الأوسع والإطار القانوني: القانون العام الأوروبي لحماية البيانات (GDPR)
- حقوق مواضيع البيانات؛ التزامات مراقبي البيانات

← تمرين: تعيين البيانات

← تمرين: سيناريوهات حمايات البيانات وتحفيز الناس للتفكير في الكيفية التي سيستجيبون بها. تحفيز الناس للتفكير في السيناريوهات الممكنة في سياقهم.

12:30: غداء (60 دقيقة)

13:30-15:00 (1.5 ساعة)

مواصلة GDPR

- طلبات وصول المواضيع – ما هي وكيف تمتثل

← تمرين: الامتثال لطلبات وصول المواضيع، معلومات الأطرف الثالثة، التنقيح

← تمرين: سيناريوهات حماية البيانات

15:00: راحة (15 دقيقة)

15:15-16:30 (1.25 ساعة)

irct
International Rehabilitation Council for Torture Victims

Ministry of Foreign Affairs of the Netherlands

مواصلة التمرينات، تحفيز المشاركين للمحاولة والتفكير في مجموعات بيانات حقيقية ترتبط بعملهم اليومي، وسيناريوهات حقيقية ترتبط بعملهم اليومي.

فكر في اتخاذ قرار على أساس الأخطار

16:30: تلخيص لليوم ولمحة عن موضوعات اليوم التالي

اليوم الثاني

10:30-09:00 (1.5 ساعة)

تلخيص لموضوعات اليوم السابق

مقدمة لإدارة البيانات المسؤولة

- ما RDM (إدارة البيانات المسؤولة)؟
- لماذا نريد أن نمارس إدارة بيانات مسؤولة/أخلاقية؟
- الاعتبارات في RDM
- السرية، التكامل، الإتاحة

← تمرين: سيناريو ومناقشة

10:30: راحة (15 دقيقة)

12:15-10:45 (1.5 ساعة)

دورة حياة البيانات: نظرة عامة على دورة حياة البيانات

- دورة حياة عادية – الخطوات في دورة حياة البيانات والأخطار في المراحل المختلفة
- الجمع، التخزين، التعامل مع، الاستخدام – الخطوات الـ 8 ضمن هذا الإطار
- I. الجمع: جمع البيانات المسؤولة
  - نظرة عامة على التخطيط، أشياء تفكر فيها عن تخطيط البيانات أو مشروع أو خدمة جديدة، تقييمات تأثيرات الخصوصية، الموافقة المدروسة، التأكد من المهارات المناسبة لدى جامعي البيانات، مجموعات البيانات القياسية
  - تقييم الخطر في إدارة البيانات المسؤولة – الاستعداد لسيناريوهات أسوأ الحالات / التعلم من الآخرين

← تمرين: ضع خطة: فكر في نشاط خدمة أساسية أو مشروع جديد، وكيف يمكنك أداء تقييم تأثير خصوصية بشأن البيانات التي تجمعها. تذكر أن تفكر في الاختلافات بين البيانات الشخصية (Pd) والبيانات غير الشخصية (non-Pd)

← تمرين: نفذ تقييم أخطار

- تدريب فريق عملك
- الموافقة: مدروسة، مناسبة، مرنة. الموافقة المدروسة: ما هي، كيف يبدو شكلها، ما الغرض من الجمع، التخطيط لسحب الموافقة أو إذا غير الناس آراءهم

← تمرين: ابتكر نموذج موافقة الذي سيقدم إلى الناس الذين يصلون إلى خدماتك عند نقطة الوصول. وستحتاج إلى التفكير في كيفية بيان الغرض الذي ستستخدم من أجله المعلومات، ولماذا تحتاج إليها.

← تمرين: ممارسة الحصول على موافقة مدروسة

12:15 - تلخيص ولمحة عن موضوعات اليوم الثالث

اليوم الثالث

11:00-09:30 (1.5 ساعة)

تلخيص الموضوعات التي تم تغطيتها حتى الآن / أسئلة وإجابات

مواصلة دورة حياة البيانات

- II. التعامل مع وIII. التخزين
  - إدارة البيانات. التأكد من تكامل البيانات، جودة البيانات، التقييس، الصحة، إمكانية المقارنة، كيفية ارتباط ذلك بالبيانات الأخلاقية. تجهيز البنية التحتية المناسبة؛ الوصول المراقب، التخزين الآمن (مادي/إلكتروني)، المشاركة/النقل الآمن – إخفاء هوية البيانات، إخفاء الهوية باستخدام بيانات مستعارة. التشفير. (ارجع إلى طلب وصول موضوع في اليوم الأول).

← تمرين: تنقية البيانات

  - مواصلة إدارة البيانات

← تمرين: اتفاقيات مشاركة البيانات

← تمرين: السيناريوهات/أشياء لتفكر فيها

11:00: راحة

12:30-11:15 (1.25 ساعة)

- IV. استخدام البيانات المسؤولة
  - الاستخدام: بيانات← معلومات← إجراء: ممارسة الضغط، الدعم، تقييم البرنامج. تحسين الجودة. التغيير. التفكير في كيفية *إساءة* استخدام البيانات

فيما تستخدم البيانات؟ كيف تضمن عدم إساءة استخدامها؟

  - الملاحظات: تقديم الملاحظات حيثما يمكن بإبلاغ الأشخاص الذين يملكون البيانات بإكمال المهمة وتقديم النتائج والتحليل لهم – تعريفهم بما حدث/ماذا تم إنجازه.

← تمرين: كيف يمكنك تقديم ملاحظات للناس الذين يستخدمون خدماتك عن ما أنجزته ببياناتهم؟ (فكر في مشاركة التقرير، أو مشاركة نتائج ممارسة الضغط – وسائل الإعلام الممكنة: مجموعات/موقع ويب)

غداء (60 دقيقة)

14:30-13:30 (ساعة واحدة)

  - الاحتفاظ والتخلص من البيانات – سياسات الاحتفاظ بالبيانات والعمليات المناسبة المتبعة. آثار البيانات - فهم موقع بياناتك: محليا/شبكات/سحابة. ربط الاحتفاظ بالبيانات بطلب وصول موضوع

← تمرين: جهز جدولا زمنيا للاحتفاظ بالبيانات للنماذج السابقة للبيانات التي تحتفظ بها

- تضمين إدارة البيانات المسؤولة في مؤسستك

← تمرين: طور خطة عمل للكيفية التي ستنقل بها المهارات التي تعلمتها على مدار الأسبوع الماضي وتطبيقها

راحة (15 دقيقة)

15:45- 14:45 (ساعة واحدة)

- مواصلة تخطيط الإجراء
- ملاحظات للمجموعة عن تقدم خطة عملك

16:00-15:45 تلخيص، أخر أسئلة وإجابات