هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

دليل تقييم مخاطر الخصوصية لمقدمي خدمات الاتصالات وتقنية المعلومات والبريد

الإصدار: 1.1
التاريخ: ديسمبر 2020 م
التصنيف: عام

citc.gov.sa

قائمة المحتويات

قائمة الجداول

1 مقدمة

وفقاً لتنظيم هيئة الاتصالات وتقنية المعلومات، وإلى نظام الاتصالات ولائحته التنفيذية، وإلى قرار مجلس الوزراء رقم (403) وتاريخ 1440/7/12هـ، الذي أسند لهيئة الاتصالات وتقنية المعلومات المهام التنظيمية والرقابية على قطاع البريد، واستناداً إلى قرار الهيئة بالرقم (416) وتاريخ 1441/9/12 هـ ، باعتماد " إجراءات إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية"، أعدت الهيئة وثيقة "دليل تقييم مخاطر الخصوصية لمقدمي خدمات الاتصالات وتقنية المعلومات والبريد".

تهدف هذه الوثيقة إلى تقديم إرشادات حول عملية تقييم مخاطر الخصوصية في الخدمات والمنتجات لمقدمي خدمات الاتصالات وتقنية المعلومات والبريد، وذلك لتوضيح عملية تقييم مخاطر الخصوصية وما تحتوي عليه بشكل أساسي لمقدمي الخدمة لاستيفاء متطلبات الخصوصية المعتمدة.

وعملية تقييم مخاطر الخصوصية هي المتطلب الأساسي المطلوب من مقدمي الخدمة عند إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية، حسب وثيقة "إجراءات إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية".

وتعد هذه الإرشادات مرجع إرشادي غير شامل، حيث توضح الحد الأدنى المناسب لاستيفاء متطلبات التنظيمات ذات العلاقة فيما يتعلق بتنفيذ عملية تقييم مخاطر الخصوصية.

المصطلحات الواردة في هذا الوثيقة، ينطبق عليها التعاريف الواردة في "إجراءات إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية".

2 عملية تقييم مخاطر الخصوصية

تتمحور عملية تقييم مخاطر الخصوصية؛ حول تحديد المخاطر المحتملة عند اجراء عمليات معالجة البيانات الشخصية وإعداد آلية لمعالجة هذه المخاطر وتقليلها؛ وتتضمن العملية عدة جوانب، يتم أخذها بعين الاعتبار، منها، مخاطر عدم الالتزام بالأنظمة أو التشريعات ذات العلاقة بالخصوصية، وحقوق أصحاب البيانات الشخصية، واحتمالية التأثير السلبي على الأشخاص أو المجتمع بشكل عام.

وتجدر الإشارة بأن عملية تقييم مخاطر الخصوصية، عملية مستمرة، حيث يتم بشكل مستمر مراجعة التقييم والتأكد من حداثته وشموليته، ومراعاة كافة المستجدات في جميع الخطوات، وانعكاسها على نتائج التقييم ومناسبة القرارات المتخذة حياله، ويشمل ذلك التأكد من التالي:

1. حداثة معلومات طبيعة المعالجة ونطاقها والغرض ومسوغاتها، وضرورة وتناسب المعالجة.
2. تغطية جميع المخاطر ذات العلاقة بآلية المعالجة المرتبطة بالبيانات الشخصية.
3. الالتزام بالأنظمة والتشريعات الصادرة من الهيئة او الجهات الأخرى ذات العلاقة بالخصوصية.

2.1. تحديد مدى الحاجة للقيام بعملية تقييم مخاطر الخصوصية:

لا يوجد حاجة لإجراء عملية تقييم مخاطر الخصوصية بالكامل حسب الحالات المذكورة في وثيقة "معايير تحديد مدى الحاجة للقيام بعملية تقييم مخاطر الخصوصية"[1].

وفي حال عدم الحاجة فإنه يكتفى بتحديد المعلومات الأساسية كالغرض والمسوغ وتقييم الضرورة والتناسب لنطاق وطبيعة المعالجة، وذكر الخدمة المشابهة، وذلك في نموذج الإشعار الموجود في ملحق (2) ويرفع للهيئة.

[1] للوصول للنسخة الأخيرة من الوثيقة والوثائق الأخرى ذات العلاقة يمكن زيارة صفحة خصوصية البيانات الشخصية على موقع الهيئة: https://www.citc.gov.sa/privacy

2.2. الأدوار والمسؤوليات:

لتنفيذ عملية تقييم مخاطر الخصوصية، ينبغي مشاركة كافة الأطراف ذات العلاقة بمعالجة البيانات الشخصية، وذلك توفير المعلومات اللازمة، بالإضافة إلى اتخاذ الإجراءات والقرارات الملائمة لمعالجة وقبول المخاطر، وذلك حسب الحالات التالية:

- في حال إطلاق خدمات أو منتجات جديدة أو إجراء تعديل على خدمات أو منتجات حالية قائمة على البيانات الشخصية:
  - يعد مقدم الخدمة مسؤول بشكل كامل عن اجراء كامل عملية تقييم مخاطر الخصوصية.

- في حال مشاركة البيانات الشخصية:
  - مع جهة تقوم بالمعالجة نيابةً عن مقدم الخدمة لأغراض يحددها مقدم الخدمة: تشارك الجهة التي سيتم مشاركة البيانات معها في توضيح تفاصيل وصف جميع أنواع المعالجة، تحديد الإجراءات الأمنية، بالإضافة إلى تقييم المخاطر ومعالجتها.
  - مع جهة لأغراض تحددها الجهة طالبة البيانات: تشارك الجهة التي سيتم مشاركة البيانات معها في كامل عملية تقييم مخاطر الخصوصية بما فيها تحديد الغرض والنطاق للمعالجة ومسوغها النظامي وتقييم ضرورتها وتناسبها.

الجدول التالي يقدم ملخصًا لأدوار الأطراف ذات العلاقة بمعالجة البيانات الشخصية في خطوات عملية تقييم مخاطر الخصوصية (✓ له دور في تنفيذ الخطوة، ✗ ليس له دور في تنفيذ الخطوة):

الحالات	الخطوات الأساسية لتقييم مخاطر الخصوصية	مقدم الخدمة	الجهة المُشارك معها
إطلاق خدمات أو منتجات قائمة على البيانات الشخصية	تحديد الغرض والنطاق للمعالجة ومسوغها النظامي وتقييم ضرورتها وتناسبها	✓	
	تحديد البيانات وطبيعتها وحساسيتها	✓	
	وصف جميع أنواع المعالجة، تحديد الإجراءات الأمنية، بالإضافة إلى تقييم المخاطر ومعالجتها	✓	
مشاركة بيانات لأغراض مقدم الخدمة	تحديد الغرض والنطاق للمعالجة ومسوغها النظامي وتقييم ضرورتها وتناسبها	✓	✗
	تحديد البيانات وطبيعتها وحساسيتها	✓	✗
	وصف جميع أنواع المعالجة، تحديد الإجراءات الأمنية، بالإضافة إلى تقييم المخاطر ومعالجتها	✓	✓
مشاركة بيانات لأغراض الجهة المُشارك معها	تحديد الغرض والنطاق للمعالجة ومسوغها النظامي وتقييم ضرورتها وتناسبها	✓	✓
	تحديد البيانات وطبيعتها وحساسيتها	✓	✓
	وصف جميع أنواع المعالجة، تحديد الإجراءات الأمنية، بالإضافة إلى تقييم المخاطر ومعالجتها	✓	✓

جدول 1: ملخص الأدوار والمسؤوليات

2.3. لجنة تقييم مخاطر الخصوصية:

يتم تقييم مخاطر الخصوصية من قبل مختصين في هذا المجال لرفع دقة نتائج التقييم والوصول للهدف منه، فيما يلي الأعضاء المقترح اشراكهم - كحد أدنى - في تقييم مخاطر الخصوصية (المسميات والمهام قد تختلف حسب المعتمد لدى مقدم الخدمة):

مسمى العضو	المهام/ المهارات
قائد فريق تقييم مخاطر الخصوصية (PIA lead)	قائد فريق تقييم مخاطر الخصوصية على البيانات الشخصية، يعتمد التقرير النهائي لتقييم مخاطر الخصوصية
مدير مشروع (Project Manager)	المسؤول الأول عن إدارة وتنفيذ المشروع المتعلق بعمليات معالجة البيانات الشخصية
أخصائي تحليل بيانات/ منفذ المعالجة (Data Processor)	المسؤول عن تنفيذ ومعالجة البيانات الشخصية
مسؤول خصوصية البيانات (Privacy Specialist)	المسؤول عن تطبيق أسس ومبادئ الخصوصية، يتطلب الإلمام بأسس ومبادئ المحافظة على خصوصية البيانات الشخصية وتنظيماتها
أخصائي قانوني (Legal Specialist)	المسؤول عن التدقيق القانوني ومتابعة الالتزام بالتنظيمات ذات العلاقة، يتطلب الإلمام بالجوانب القانونية والتنظيمات والقرارات ذات العلاقة

جدول 2: لجنة تقييم مخاطر الخصوصية

هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

عملية تقييم مخاطر الخصوصية (Privacy Impact Assessment)

«الخطوات التفصيلية»

citc.gov.sa

3 الخطوات التفصيلية لإجراء عملية تقييم مخاطر الخصوصية

تبدأ عملية تقييم مخاطر الخصوصية بالقيام بمراجعة الوثائق ذات العلاقة بالمشروع المتعلق بعمليات المعالجة للبيانات الشخصية، لتنفيذ الفقرات التالية، وقد تشمل هذه الوثائق، خطة المشروع، العقود بين الجهات الأخرى، تقارير التقييم الفنيَّة، والمواصفات الوظيفية للأنظمة المستخدمة وغيرها. الرسم التوضيحي التالي يوضح الخطوات التفصيلية لإجراء عملية تقييم مخاطر الخصوصية.

1. تحديد الغرض (Purpose of Processing)
2. تحديد المسوغ النظامي (Legal Bases)
3. تحديد نطاق المعالجة (Scope of Processing)
4. الموازنة بين ضرورة المعالجة وتناسبها مع الفائدة المرجوة (Necessity and Proportionality)
5. تحديد البيانات وطبيعتها وحساسيتها (Categories of Data)
6. وصف جميع أنواع المعالجة (من الجمع والإنشاء حتى الإتلاف) (Nature of Processing)
7. تحديد الضوابط الأمنية المخطط تنفيذها (Envisaged Security Controls)
8. تحديد وتقييم المخاطر (مخاطر انتهاك الخصوصية) (Privacy Risk Assessment) :

المخاطر (Risks)	درجة الضرر المحتمل على الخصوصية (Severity Of Impact)	احتمالية الخطر (Risk Likelihood)	احتساب درجة الخطر الكلية (Total Risk Values)	معالجة المخاطر (Addressing Risks)	درجة المخاطر بعد المعالجة (Residual Risk Values)

9. التوثيق (Documentation)

تقرير تقييم مخاطر الخصوصية (Privacy Impact Assessment Report)

المراجعة والتقييم الدوري (Periodic Review and Assessment)

شكل 1: الخطوات التفصيلية لإجراء عملية تقييم مخاطر الخصوصية.

3.1. تحديد الغرض (Purpose of Processing):

يتم تحديد الغرض من معالجة البيانات الشخصية، ويشمل ذلك توضيح المصلحة المتحققة من تنفيذ عمليات المعالجة والفائدة المتوقع تحققها لأصحاب البيانات وللمجتمع ككل، وتختلف الجهة المسؤولة عن تحديد الغرض حسب التالي:

- يتم تحديد الغرض من قبل مقدم الخدمة في الحالات التالية:
  - إطلاق خدمات أو منتجات قائمة على البيانات الشخصية
  - مشاركة البيانات الشخصية مع جهة تقوم بالمعالجة نيابةً عن مقدم الخدمة لأغراضه.
- بينما يتم تحديد الغرض من قبل الجهة طالبة البيانات في حالة مشاركة البيانات الشخصية مع جهة لأغراض تحددها تلك الجهة.

الجهة التي تحدد الغرض هي الجهة التي تتحقق لها المصلحة من معالجة البيانات، وتعد الجهة المعنية بشكل أساسي بتقييم مخاطر الخصوصية واستيفاء متطلبات الخصوصية

2.3. المسوغ النظامي (Legal Bases):

يتم توضيح المسوغ النظامي لمعالجة البيانات، إما بموافقة صاحب البيانات على الغرض المحدد، أو وجود أسس نظامية أخرى مستثناة من الموافقة.

3.3. نطاق المعالجة (Scope of Processing):

يتم تحديد نطاق البيانات الشخصية التي سيتم معالجتها، ونطاق المعالجة، وتقييم مدى الحاجة لها، أو استبعادها إن اتضح عدم الحاجة لها؛ ومن ذلك، يتم تحديد:

- طبيعة أصحاب البيانات: على سبيل المثال: (النطاق العمري، وجود فئات حساسة كالأشخاص ذوي الإعاقة، أو الضعفاء، أو الأطفال).
- الطبيعة العامة للبيانات الشخصية، على سبيل المثال: (رقمية، ورقية، مُجمعَّة، موزَّعة).
- المدة المتوقعة لمعالجة البيانات الشخصية.
- الأنظمة المتعلقة بالبيانات الشخصية والمعتمدة عليها، سواء أكانت تلك الأنظمة (برامج، او شبكات، أو اشخاص، أو غيرها).
- حجم البيانات الشخصية: على سبيل المثال: (عدد الأشخاص، عدد السجلات، المحيط الجغرافي).
- وتيرة وعمق عمليات المعالجة البيانات الشخصية.

شكل 2: تحديد نطاق المعالجة.

3.4. الموازنة بين ضرورة المعالجة وتناسبها مع الفائدة المرجوة (Necessity and Proportionality):

يتم تقييم مدى ضرورة المعالجة لتحقيق الغرض وعلاقته بها، وتناسبها مع الفائدة المرجوة من عمليات المعالجة، أخذًا بالاعتبار نطاقها وطبيعتها، ودراسة الطرق الأخرى البديلة الممكنة لتحقيق الغرض دون اللجوء لمعالجة بيانات شخصية.

3.5. تحديد البيانات وطبيعتها وحساسيتها (Categories of Data):

يتم تحديد البيانات الشخصية المستخدمة في المعالجة بدقة، ويتم تحديد أنواعها، وتحديد مدى حساسية هذه البيانات. ويؤخذ بعين الاعتبار عند تحديد حساسية البيانات كونها ذات ارتباط مباشر أو غير مباشر بأصحاب البيانات، حيث تعرف البيانات الشخصية بمعرفات مباشرة إذا كانت تدل بشكل مباشر على هوية الشخص، وغيرها بمعرفات غير مباشرة.

أمثلة على المعرفات المباشرة وغير المباشرة:

المعرفات	أمثلة
معرفات مباشرة	الاسم، الصور الشخصية، البصمات، أرقام السجلات (الهوية الوطنية، رقم الجواز، رقم الرخصة، رقم الحساب البنكي)، البطاقة الائتمانية، رقم التواصل، عنوان المنزل، سلوك الاستخدام للمستخدم، المعرف الرقمي (IP)، البريد الالكتروني، بيانات صحية.
معرفات غير مباشرة	العمر، الجنس (ذكر، انثى)، الدرجة العلمية، الراتب، الوظيفة، التواريخ المرتبطة (تاريخ الميلاد، الاشتراك، انتهاء خدمة)، أسم مستخدم مستعار، مكان الميلاد، مكان الوظيفة.

جدول 3: المعرفات المباشرة وغير المباشرة

كما يؤخذ بعين الاعتبار البيانات ذات الطبيعة الحساسة من حيث تأثيرها المحتمل على الشخص، ومن ذلك على سبيل المثال: البيانات المكانية؛ وهي البيانات التي تحدد موقع الشخص وتنقلاته، وبيانات التتبع ومراقبة سلوك المستخدم؛ والتي تجمع بوسائل مختلفة لتكوين ملفات للمستخدمين عبر الشبكات والخدمات (على سبيل المثال البيانات التي تجمع بالتقنيات التالية: - Fingerprinting – Cross Device Tracking (Cookies

يتم تحديد قيمة الضرر الأعلى عند التعامل او معالجة المعرفات المباشرة مقارنةً بغير المباشرة، وعند التعامل مع البيانات ذات الطبيعة الحساسة

3.6. وصف جميع أنواع المعالجة (من الجمع والإنشاء حتى الإتلاف) (Nature of Processing):

في هذه المرحلة يتم تحديد كيفية جمع البيانات الشخصية، ومعالجتها؛ حيث يتم توضيح آلية تدفقها بمراحل المشروع المتعلق بعمليات المعالجة، من جمعها حتى إتلافها، وتشمل هذه المراحل بحد أدنى التالي:

شكل 3 : مراحل معالجة البيانات

لتوضيح المراحل أعلاه، تم استعراض مثال افتراضي في ملحق (3) يوضح آلية استخدام دورة حياة تدفق البيانات لوصف جميع أنواع المعالجة

3.7. تحديد الضوابط الأمنية المخطط تنفيذها (Envisaged Security Controls):

تحديد الضوابط الأمنية المخطط تنفيذها اثناء معالجة البيانات الشخصية، مع تقديم الأدلة الداعمة، ومنها على سبيل المثال:

- المعايير المعتمدة للمحافظة على خصوصية أصحاب البيانات الشخصية.
- الإجراءات والوسائل المتخذة لضمان حقوق أصحاب البيانات الشخصية.
- المعايير المعتمدة لمراقبة الامتثال والالتزام بالمحافظة على خصوصية البيانات الشخصية.

3.8. تحديد وتقييم المخاطر (مخاطر انتهاك الخصوصية) (Privacy Risk Assessment):

تعد هذه الخطوة هي الخطوة الأساسية لإحصاء كافة أنواع المخاطر على الخصوصية واحتساب درجاتها وتصنيفها، ويمكن تنفيذ ذلك بإعداد قائمة، على النحو التالي:

3.8.1. المخاطر (Risks):

في تحديد المخاطر ينبغي اعتبار أي تأثير محتمل على أصحاب البيانات، وأي أذى أو ضرر يمكن أن ينتج من المعالجة، سواءً جسديًّا، أو معنويًّا، أو ماديًّا، على وجه الخصوص، ينبغي النظر فيما إذا كانت المعالجة تؤدي لأي من التالي:

- عدم القدرة على ممارسة الحقوق (تشمل الحقوق ذات العلاقة بالخصوصية وغيرها).
- عدم القدرة على الوصول إلى الخدمات أو الإمكانيات.
- فقدان القدرة على التحكم بالبيانات الشخصية واستخدامها.
- العنصرية والتمييز بجميع أشكاله.
- سرقة الهوية أو تزويرها.
- الخسارة المادية.
- إضرار بالسمعة.
- الضرر الجسدي.
- انعدام السريَّة/ فقدان السريَّة
- إعادة تعريف الهوية من بيانات مخفية الهويَّة.
- أي نوع من أنواع الحرمان الاجتماعي.

يمكن الاستعانة بالخطوات الارشادية الموضحة أدناه؛ لتحديد المخاطر ذات العلاقة (قائمة غير شاملة):

- تحديد المتطلبات النظامية للمحافظة على خصوصية البيانات الشخصية وإمكانية الالتزام بكلٍّ منها.
- تحديد أفضل الممارسات العالمية في المحافظة على خصوصية البيانات الشخصية وإمكانية تطبيق كلٍّ منها.
- تحديد الفجوات الممكنة في عمليات المعالجة/تدفق البيانات التي قد تؤدي إلى عدم الالتزام بمتطلبات المحافظة على خصوصية البيانات الشخصية (مثلًا: تؤدي إلى تسريب البيانات).
- هل العاملين على معالجة البيانات على معرفة كاملة بأدوارهم ومسؤولياتهم؟
- هل تم توعية وتدريب العاملين بالسياسات والممارسات المعتمدة للمحافظة على خصوصية البيانات الشخصية؟
- هل تم توعية الأطراف الخارجية بالتزاماتهم للمحافظة على خصوصية البيانات الشخصية؟
- كما ينبغي تحديد مخاطر وتهديدات الأمن السيبراني وتحديد المصادر الممكنة لها، بما في ذلك: الدخول غير المشروع/ غير المصرح به، والتعديل غير المشروع للبيانات وفقدان البيانات.

تم استعراض طريقة مقترحة لتحديد قائمة المخاطر في مثال افتراضي في ملحق (4) يستعرض تصنيفات مقترحة وأسئلة لتحديد المخاطر.

3.8.2. درجة الضرر المحتمل على الخصوصية (Severity Of Impact):

بعد تحديد المخاطر يتم قياس وتحليل ضررها المتوقع على أصحاب البيانات، بحيث تُقدر قيمة للضرر بناء على إطار المخاطر المعتمد لدى مقدم الخدمة، يتم تحديد الضرر من ضرر بالغ الشدة إلى ضرر منخفض أو معدوم وبتسلسل مناسب.

يؤخذ بعين الاعتبار عند تقدير قيمة الضرر الفئات الأكثر حساسية من أصحاب البيانات: على سبيل المثال الأطفال، والأشخاص ذوي الإعاقة، والضعفاء وغيرهم.

مثال لمستويات الضرر المتوقع:

- ضرر بالغ الشدة: عواقب وخيمة، وتدل المؤشرات على احتمالية منخفضة إلى معدومة لتصحيحها أو تجاوزها.
- ضرر شديد: عواقب واسعة النطاق، تطال خسائر مادية أو معنوية.
- ضرر متوسط: عواقب سلبية، وتدل المؤشرات على إمكانية تجاوزها خلال فترة قصيرة.
- ضرر بسيط: عواقب سلبية، لكن لا توجد مؤشرات لحصول خسائر مادية أو معنوية.
- ضرر منخفض أو معدوم: عواقب مستبعدة إلى معدومة.

3.8.3. احتمالية الخطر (Risk Likelihood):

تحتسب احتمالية حدوث الخطر بناء على إطار المخاطر المعتمد لدى مقدم الخدمة، أخذًا في الاعتبار طبيعة المعالجة والتدابير المتخذة وكافة العوامل ذات العلاقة، يتم تحديد الاحتمالية من حتمي الحدوث إلى مستبعد وبتسلسل مناسب.

مثال لمستويات احتمالية الخطر:

- شبه مؤكد: توجد مؤشرات كافية لاحتمالية مرتفعة بحدوثه على المدى القريب.
- متوقع: توجد مؤشرات كافية لتوقع حدوثه على المدى القريب.
- ممكن: توجد مؤشرات كافية لإمكانية حدوثه على المدى القريب.
- غير متوقع: يمكن حدوثه لكن لا توجد مؤشرات أو أدلة لحدوثه على المدى القريب.
- مستبعد: نادر الحدوث، ولا يمكن تصور حدوثه.

في الخطوتين السابقتين 3.8.2 و 3.8.3 من المهم تحديد القيم بناء على الحقائق والتوقعات الواقعية وبالاستعانة بآراء ذوي الخبرة والاختصاص، حيث يتم الأخذ بعين الاعتبار الثغرات الممكنة ، إمكانيات مصادر التهديد، والعوامل الاجتماعية، والنظامية، والفنية المتعلقة بسياق المعالجة عند تقييم احتمالية المخاطر.

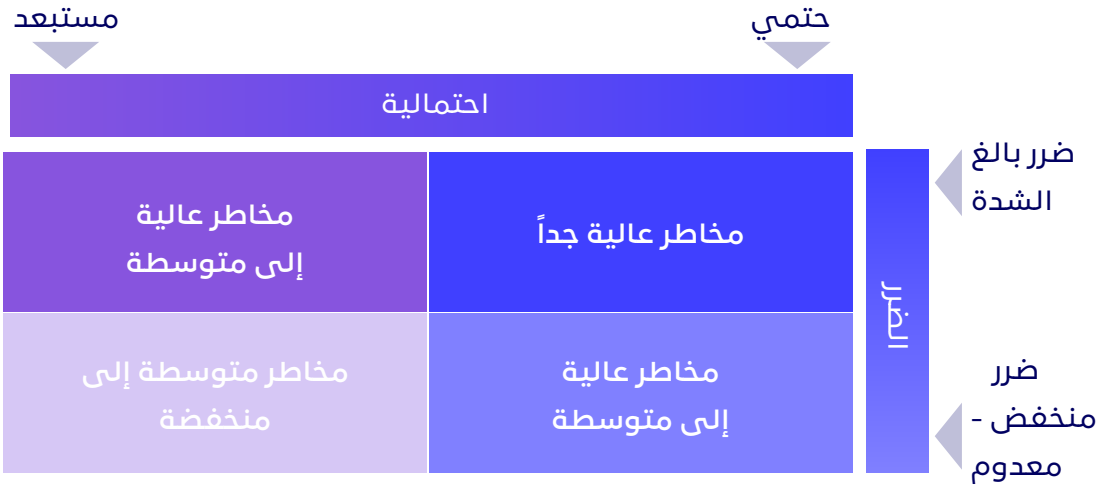
في الخطوتين السابقتين3.8.2 و 3.8.3 يتضح أثر الضوابط الأمنية المخطط تنفيذها (كما في الخطوة 7.3) في تقليل احتمالية الخطر أو أثره

3.8.4. احتساب درجة الخطر الكلية بناء على درجة الضرر واحتمالية حدوثه (Total Risk Values)

بعد تحديد درجة الضرر المتوقع على حقوق وحريات أصحاب البيانات، واحتساب احتمالية حدوث الخطر؛ تحسب قيمة كلية للخطر ويتم تصنيفه من مخاطر عالية جدًا إلى مخاطر منخفضة مستبعدة وبتسلسل مناسب.

المخاطر العالية جدًا يمكن أن تنتج من احتمالية حدوث خطر مرتفعة لخطر بأضرار منخفضة، أو من احتمالية حدوث خطر أقل بضرر بالغ الشدة.

الجدول التالي يوضح بشكل مبسط تصنيف للمخاطر بناء على درجة الضرر واحتمالية الخطر.



جدول 4 : توضيح تصنيفات المخاطر والأضرار

يُحدد معيار احتساب قيمة الخطر وتصنيفه بناءً على إطار المخاطر المعتمد لدى مقدم الخدمة، يشمل هذا المعيار آلية احتساب القيم لكل مستوى من مستويات الأثر المتوقع ومستويات احتمالية الخطر، وكيفية استنتاج قيمة الخطر الكلية منها، كما يُحدد فيه معيار قبول الخطر.

ينبغي تبني الإطار الملائم لإدارة المخاطر بما يتناسب مع طبيعة أعمال الجهة ومراعاة المتطلبات القانونية والتنظيمية المختلفة، والأخذ بأفضل الممارسات العالمية في إدارة المخاطر

مثال توضيحي لاحتساب درجة المخاطر:

يمكن احتساب درجة الخطر الكلية بناءً على إطار المخاطر وذلك باعتماد قيم لمستويات الضرر المتوقع ومستويات احتمالية الخطر كالمثال التالي:

- مقياس مستويات الضرر المتوقع:

القيمة	المستوى	وصف المستوى
5	ضرر بالغ الشدة	عواقب وخيمة، وتدل المؤشرات على احتمالية منخفضة إلى معدومة لتصحيحها أو تجاوزها
4	ضرر شديد	عواقب واسعة النطاق، تطال خسائر مادية أو معنوية
3	ضرر متوسط	عواقب سلبية، وتدل المؤشرات على إمكانية تجاوزها خلال فترة قصيرة
2	ضرر بسيط	عواقب سلبية، لكن لا توجد مؤشرات لحصول خسائر مادية أو معنوية
1	ضرر منخفض أو معدوم	عواقب مستبعدة إلى معدومة

جدول 5 : مستويات الضرر

- مقياس مستويات احتمالية الخطر:

القيمة	المستوى	وصف المستوى
5	شبه مؤكد	توجد مؤشرات كافية لاحتمالية مرتفعة بحدوثه على المدى القريب
4	متوقع	توجد مؤشرات كافية لتوقع حدوثه على المدى القريب
3	ممكن	توجد مؤشرات كافية لإمكانية حدوثه على المدى القريب
2	غير متوقع	يمكن حدوثه لكن لا توجد مؤشرات أو أدلة لحدوثه على المدى القريب
1	مستبعد	نادر الحدوث، ولا يمكن تصور حدوثه

جدول 6 : مستويات احتمالية الخطر

بناءً على المقاييس أعلاه، ولكل خطر تم تحديده، وبعد تحديد درجة الضرر واحتمالية الخطر المتعلقة به، يمكن ضرب قيمة كل من مستوى الضرر ومستوى احتمالية الخطر لاحتساب درجة الخطر الكلية، قيم المخاطر في هذا المثال تتدرج على مقياس من 5 نقاط، ويعني ذلك أن أقل قيمة ممكنة للخطر = 1 بينما أعلى قيمة ممكنة = 25، وبالتالي يمكن تحديد معيار قبول المخاطر بقيمة مخاطر 15 وأدنى مثلًا، وبالتالي تعد المخاطر بقيمة أعلى من 15 غير مقبولة وذات أولوية قصوى للمعالجة.

3.8.5. معالجة المخاطر (Addressing Risks):

في هذه الخطوة يتم دراسة وتحديد الاجراءات الملائمة لمعالجة المخاطر وتقليل احتمالية حدوثها أو أثرها المتوقع، وبخاصَّة المخاطر العالية والتي تتجاوز معيار قبول المخاطر لدى مقدم الخدمة، يمكن اعتبار أحد الاجراءات التالية على سبيل المثال (القائمة أدناه غير شاملة):

- اتخاذ القرار باستثناء أنواع من البيانات الشخصية من الجمع والمعالجة.
- تقليل نطاق المعالجة.
- تقليل مدة الاحتفاظ بالبيانات الشخصية.
- إضافة المزيد من الضوابط الأمنية.
- تدريب العاملين للتأكد من توقع المخاطر وتجنبها.
- تطبيق عمليات إخفاء الهوية.
- اعتماد سياسات وإجراءات داخلية لتفادي المخاطر.
- استخدام تقنيات مختلفة.
- اعتماد وتوثيق اتفاقيات مشاركة بيانات واضحة.
- اجراء التعديلات اللازمة على سياسة الخصوصية ومشاركتها.
- إتاحة خيار سحب الموافقة لأصحاب البيانات.
- تطوير أنظمة وإجراءات لتمكين أصحاب البيانات من ممارسة حقوقهم.

3.8.6. درجة المخاطر بعد المعالجة (Residual Risk Values):

بعد اتخاذ الاجراءات الملائمة لمعالجة المخاطر يتم إعادة تقييم درجة الضرر واحتمالية الخطر واحتساب قيمة الخطر المتبقية لتقييم مناسبة الإجراءات المتخذة وأثرها على قيمة المخاطر. في هذه الخطوة يتم الخلوص إلى النتيجة النهائية لتقييم المخاطر بتحديد المخاطر وقيمها المتبقية ومقارنتها بالنسبة المقبولة للمخاطر وتوثيق خطة العمل التنفيذية لإجراءات معالجة المخاطر المتخذة في الخطوة السابقة مع تضمين الأدلة الداعمة.

في حال وجود مخاطر تتجاوز معيار قبول المخاطر، بعد الخطوتين السابقتين فمن الأجدر إعادة النظر في عملية المعالجة والحاجة لها

3.9. التوثيق (Documentation):

يتم توثيق المراحل المتبعة لتقييم مخاطر الخصوصية عند البدء في عملية تقييم مخاطر الخصوصية وعند كل مرحلة، ويشمل جميع الخطوات السابقة، بالإضافة إلى مسببات قبول مخاطر الخصوصية، والإجراء المتخذ، والأشخاص المخولين لاتخاذ قرار قبول نتيجة المخاطر من عدمه وغيرها.

من المهم توثيق كافة الخطوات ومراحل تنفيذها ونتائجها بشكل تفصيلي، للتأكد من توفر المعلومات الكاملة عند الحاجة لها لإعادة التقييم أو عند طلب الجهات المعنية

3.9.1. تقرير تقييم مخاطر الخصوصية (Privacy Impact Assessment Report):

في مرحلة التوثيق يتم إعداد التقرير بالمحتويات الواردة في ملحق (1)، لرفعه إلى الهيئة وتوفير أي معلومات إضافية عند الحاجة، كما يتم تحديث التقرير عند المراجعة والتقييم الدوري كما سيرد في القسم (3.10)، وفي حال تغير نتائج التقييم يعاد رفع التقرير المحدث للهيئة.

3.10. المراجعة والتقييم الدوري (Periodic Review and Assessment):

يتم مراجعة عملية تقييم مخاطر الخصوصية بشكل دوري وعند حدوث أي تغيير على طبيعة المعالجة، أو نطاقها، أو سياقها، أو أغراضها، أو طريقة تنفيذها، على سبيل المثال ينبغي مراجعة تقييم مخاطر الخصوصية وتحديث نتائجها في الحالات التالية:

- عند حدوث تغيير في التقنيات والوسائل المستخدمة لمعالجة البيانات الشخصية.
- عند حدوث تغيير في الضوابط الأمنية المطبقة.
- عند الحاجة للمزيد من الضوابط الأمنية بناء على ثغرات أو تهديدات مستجدة.
- عند حدوث تغيير في تنظيمات ومتطلبات الخصوصية الصادرة من الجهات المختصة.

هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

الملاحق

citc.gov.sa

ملحق (1): محتويات تقرير تقييم مخاطر الخصوصية

تستخدم هذه القائمة للتحقق من شمولية تقرير تقييم مخاطر الخصوصية على الحد الأدنى من المحتوى المطلوب وذلك لاستيفاء متطلبات البند 4-3 من إجراءات إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية المعتمدة بقرار رقم 416 وتاريخ 1441/9/12هـ، يتم تعبئتها وإرفاقها مع التقرير المعد حسب دليل تقييم مخاطر الخصوصية بعد اعتماد قائد فريق تقييم مخاطر الخصوصية (PIA lead).

تفاصيل التقرير	مرفق
مقدمة مختصرة عن أهداف المشروع، والمعالجة المتضمنة، ولماذا دعت الحاجة للقيام بتقييم مخاطر الخصوصية	☐
وصف للغرض من معالجة البيانات الشخصية المحددة ومسوغها المشروع، والمصلحة المتحققة نتيجة عمليات المعالجة والفائدة المتوقع تحققها لأصحاب البيانات وللمجتمع	☐
وصف لنطاق البيانات الشخصية التي سيتم معالجتها، ونطاق المعالجة، ونتيجة تقييم الضرورة والتناسب	☐
وصف للبيانات الشخصية وعمليات معالجة البيانات، مثل كيفية جمع البيانات، واستخدامها، وتخزينها، والتخلص منها، ومصدر البيانات، وهل سيتم مشاركتها مع أطراف أخرى. (يمكن ارفاق رسم بياني لذلك)	☐
وصف للضوابط الأمنية المخطط تنفيذها، مع تقديم الأدلة الداعمة	☐
تفاصيل المخاطر واحتماليتها وضررها المتوقع والدرجات الكلية لها	☐
إجراءات معالجة المخاطر المعتمدة	☐
نسبة الخطر المتبقية ومبررات قبولها، ومعلومات الشخص المخول بقبولها	☐
معلومات لجنة تقييم مخاطر الخصوصية (الاسم، الدور، معلومات التواصل)	☐

اعتماد قائد فريق تقييم مخاطر الخصوصية (PIA lead)	الاسم والتوقيع

الجدول أعلاه يرفق مع التقرير، بعد اعتماده من قائد لجنة تقييم مخاطر الخصوصية

ملحق (2): نموذج إشعار الهيئة بإطلاق خدمات أو مشاركة بيانات شخصية

يستخدم هذا النموذج لإشعار الهيئة قبل إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية حسب البند 4-2 من إجراءات إطلاق خدمات أو منتجات معتمدة على البيانات الشخصية للمستخدمين أو مشاركة البيانات الشخصية المعتمدة بقرار رقم 416 وتاريخ 1441/9/12هـ. يتم تعبئة فقرات النموذج حسب دليل تقييم مخاطر الخصوصية

اسم مقدم الخدمة	
التاريخ	

وصف المنتج/الخدمة أو عملية المشاركة
عمليات معالجة البيانات الشخصية
الغرض من معالجة البيانات الشخصية، والمسوغ النظامي لها
تقييم ضرورة المعالجة وتناسبها مع الفائدة المرجوة
مبرر عدم الحاجة لتقييم مخاطر الخصوصية بشكل كامل

يتم ذكر المعيار المنطبق حسب وثيقة معايير مدى الحاجة للقيام بعملية تقييم مخاطر الخصوصية

اسم مختص خصوصية البيانات		هاتف	
اعتماد قائد فريق تقييم مخاطر الخصوصية (PIA lead)	الاسم والتوقيع		

ملحق (3): مثال توضيحي (1) لخطوة وصف أنواع المعالجة

قامت الشركة -أ- باستشارة الإدارات ذات العلاقة بشأن مشروع خاص لإقامة حدث تقني كبير، والذي يتم من خلاله جمع ومعالجة بيانات شخصية، ومراجعة الوثائق لمشاريع سابقة مشابهه، وعليه فإن لجنة تقييم الأثر على البيانات الشخصية، تقوم بتحديد البيانات التي سيتم استخدامها بالمشروع والغرض من جمعها واستخدامها. ولعمل ذلك، فإن اللجنة ستحدد بشكل تفصيلي ومن خلال دورة حياة البيانات في المشروع، البيانات المستخدمة ومبررات استخدامها، والأخذ بعين الاعتبار الجوانب التالية:

1. صلاحية الاطلاع على البيانات الشخصية (داخلياً أو من أطراف خارجية).
2. مكان وكيفية تخزين البيانات الشخصية
3. آلية استخدام البيانات الشخصية.
4. مدة تخزين ومعالجة البيانات وآلية إتلافها بعد الانتهاء منها.

أدناه، ملخص توضيحي لعمل لجنة تقييم الأثر على البيانات الشخصية لهذه المرحلة:

1

جمع البيانات الشخصية

يتم تسجيل المهتمين بالمشاركة بالحدث التقني وتقديم البيانات المطلوبة على موقع الشركة -أ-، ويتم إشعارهم بالغرض المحدد من جمع البيانات الشخصية، وبإمكانهم مراجعة المزيد من التفاصيل في سياسة حماية البيانات الشخصية المنشورة في موقع الشركة -أ- الإلكتروني.

البيانات الشخصية المطلوبة	الغرض من الجمع
الاسم	التحقق من المشاركين قبل وأثناء المشاركة وبعد المشاركة في الحدث التقني
رقم الجوال البريد الالكتروني	بغرض التواصل مع المشتركين، لتقديم معلومات قبل المشاركة بالحدث التقني بيوم عن تفاصيل الحدث وبوابات الدخول وغيرها
العمر الجنس (ذكر ، انثى)	لتتبع الأحداث التقنية للمشتركين مستقبلاً، وما إذا هم مخولين للمشاركة بالمسابقات أم لا، بناء على معايير تحددها لجنة المسابقات في الحدث التقني
الصحة العامة (سليم، يعاني من مرض، تحديد)	تقديم الدعم والرعاية الصحية في وقت الحدث التقني عند الحاجة لها
أسم قريب رقم جوال القريب	عند الأحداث الطارئة، يتم التواصل مع الأقرباء
بيانات مالية	لتحصيل رسوم الاشتراك في الحدث التقني

معلومات للإجابة عليها في هذه المرحلة	
هل سيتم إشعار المشتركين بالغرض من جمع واستخدام والإفصاح عن بياناتهم الشخصية؟	نعم، سيتم اشعار المشتركين بالغرض من جمع بياناتهم واستخدامها في الموقع الالكتروني وذلك عند تسجيلهم في الموقع
كيف يتم أخذ الموافقة من المشتركين على استخدام بياناتهم الشخصية؟	عند تسجيل بياناتهم في الموقع عن طريق ايقونة (موافق) على غرض استخدام البيانات الشخصية
مصدر البيانات الشخصية (المزود)	الأشخاص المشتركين
آلية جمع البيانات الشخصية	إلكترونية من الموقع الإلكتروني

2

تخزين البيانات الشخصية

يتم تخزين البيانات الشخصية في قاعدة بيانات خاصة في الشركة -أ-، والأشخاص المخولين بصلاحية الدخول على هذه البيانات هم أشخاص محددين مختصين في الشركة -أ-.

التخزين المادي	التخزين الالكتروني
لا يوجد	عند تعبئة النماذج المطلوبة من المشتركين، يتم ارسالها لقاعدة بيانات خاصة في الشركة، وقصر صلاحية الدخول لأشخاص محددين ومختصين

3

استخدام البيانات الشخصية

تقوم الشركة -أ- باستخدام البيانات الشخصية، التي تم جمعها لأغراض محددة ادناه، وحيث أن هناك عدد من الإدارات في الشركة ستقوم باستخدام البيانات لأغراض مختلفة، سيتم منح صلاحية الدخول على البيانات الشخصية لكل إدارة أو أشخاص بناء على الحاجة لمعالجتها

الإدارة	الغرض من الاستخدام	الصلاحية الممنوحة
العلاقات العامة	بيانات التواصل مع المشتركين، لتزويدهم بالمعلومات حول أوقات الدخول وافتتاح مكان التجمع وغيرها	الصلاحية الكاملة للبيانات التي جمعها، باستثناء البيانات المالية
الإدارة المالية	المعلومات المالية	صلاحية للاسم كاملاً، وبيانات البطاقات الائتمانية لإنجاز عمليات الدفع

4

الإفصاح أو مشاركة البيانات الشخصية

تقوم الشركة -أ- بمشاركة البيانات الشخصية المحددة ادناه للأغراض المذكورة.

البيانات والغرض من مشاركتها مع الأطراف الخارجية	الطرف الخارجي وطريقة المشاركة
بيانات المشتركين وهي: الاسم، وذلك لطباعة الهدايا التذكارية لكل مشترك	سيتم مشاركة البيانات المذكورة مع الشركة -ب-، عن طريق البريد الالكتروني

5

مدة الاحتفاظ والإتلاف للبيانات الشخصية

تقوم الشركة -أ- بالاحتفاظ وإتلاف البيانات الشخصية التي تم جمعها بناء على السياسة المعمول بها في الشركة.

الاحتفاظ بالبيانات الشخصية	إتلاف البيانات
ثلاث سنوات بعد جمع البيانات الشخصية	إزالة البيانات الالكترونية من قاعدة البيانات باستخدام أدوات الحذف حسب ما هو موصى به في السياسة

ملحق (4): مثال توضيحي (2) لخطوة تحديد وتقييم المخاطر:

مجال الخطر	أمثلة مبدئية غير شاملة: الأسئلة ذات العلاقة	الإجابة ووصف الخطر، مع ذكر الأدلة ذات العلاقة	تقييم الخطر: الأثر/ الضرر	تقييم الخطر: احتمالية الخطر	تقييم الخطر: درجة الخطر الكلية
المتطلبات النظامية للمحافظة على خصوصية البيانات الشخصية	هل يتم أخذ موافقة أصحاب البيانات على الغرض من المعالجة؟	نعم، عند جمعها عبر الموقع يستعرض للمستخدم البيانات التي سيتم جمعها ومعالجتها مع خيار للموافقة، لا يتم توضيح الأطراف الخارجية التي ستشارك معها البيانات لمعالجتها	4	1	4
	هل يوجد إمكانية للتراجع عن الموافقة؟	لا يوجد إمكانية متاحة للتراجع بعد الجمع	3	2	6
	هل توجد إجراءات للتأكد من دقة وحداثة البيانات الشخصية؟	يوجد إجراءات مؤتمتة للتدقيق على تعبئة حقول البيانات كاملة، لكن لا يوجد اجراءات تحقق كافية للتحقق من الدقة، ولا يوجد وسيلة لتحقق صاحب البيانات من صحة بياناته	4	4	16
	...				
التأثير السلبي على أصحاب البيانات	هل يمكن أن تسبب المعالجة أي نوع من أنواع الحرمان الاجتماعي أو الاقتصادي لأصحاب البيانات أو فئة منهم؟				
	هل يمكن أن يفتقد أصحاب البيانات القدرة على التحكم ببياناتهم الشخصية واستخدامها؟				
	...				
الأدوار والمسؤوليات	هل تم توعية وتدريب العاملين بالسياسات والممارسات المعتمدة للمحافظة على خصوصية البيانات الشخصية؟				
	هل تم توعية الأطراف الخارجية بالتزاماتهم للمحافظة على خصوصية البيانات الشخصية؟				
	...				
مخاطر وتهديدات الأمن السيبراني	هل يمكن الاطلاع أو الوصول غير المشروع/ غير المصرح به على البيانات؟				
	...				
...	...				


CITC
هيئة الاتصالات وتقنية المعلومات
Communications & Information
Technology Commission

citc.gov.sa