1. مقدمة

1.1 الغرض

يصف توجيه السياسة هذا التدابير التي اتخذتها ACIG لحماية خصوصية موظفيها والمستفيدين (موضوع البيانات) معلومات التعريف الشخصية (PII).

1.2 النطاق

تنطبق هذه السياسة على جميع أنظمة أسيج ومعداتها وموظفيها والأطراف الثالثة التي توظفها أسيج سواء بشكل مباشر أو غير مباشر.

1.3 المصطلحات الرئيسية

المصطلح	الوصف
موضوع البيانات	الشخص الطبيعي الذي يمكن التعرف عليه هو الشخص الذي يمكن تحديده، بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرف مثل الاسم أو رقم التعريف أو بيانات الموقع أو المعرف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للهوية المادية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي (والمستفيدين ACIG بما في ذلك موظفي).
معلومات تحديد الهوية الشخصية	أي معلومات تتعلق بشخص حي طبيعي محدد أو بشخص حي طبيعي يمكن تحديده ، بشكل مباشر أو غير مباشر ، على وجه الخصوص بالرجوع إلى معرف مثل الاسم أو رقم الهوية أو بيانات الموقع أو عنوان IP أو المعرفات الأخرى عبر الإنترنت أو إلى واحد أو أكثر من العوامل الأخرى الخاصة بهوية الشخص.
المعالجة	أي عملية أو مجموعة من العمليات التي يتم إجراؤها على معلومات تحديد الهوية الشخصية أو على مجموعات من معلومات تحديد الهوية الشخصية ، سواء بوسائل آلية أم لا ، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكيف أو التغيير أو الاسترجاع أو الاستشارة أو الاستخدام أو الكشف عن طريق الإرسال أو النشر أو الإتاحة أو المحاذاة أو الدمج أو التقييد أو المحو أو التدمير.
الضابط	موظف اسيج.الذي يحدد أغراض ووسائل معالجة معلومات تحديد الهوية الشخصية

1.4 الأدوار والمسؤوليات

يجب على كبير مسؤولي أمن البيانات والمعلومات / مسؤول حماية التواريخ:

- الإشراف على الامتثال للسياسة والانتهاكات والاستثناءات وحل النزاعات.
- ضمان التوافق بين هذه السياسة وأعمال أسيج واستراتيجيتها.
- إدارة استثناءات وانتهاكات السياسة.

تختص الإدارة القانونية بما يلي:

- تحديد قوانين ولوائح الخصوصية المعمول بها على ACIG ؛
- تنفيذ دورهم في تحليل تأثير الخصوصية ؛
- تحديد متطلبات الخصوصية في عقود الأطراف الثالثة أو المستندات ذات الصلة.

يجب على مالكي البيانات / رؤساء الأقسام:

- تطبيق المتطلبات الواردة في هذه السياسة على معلومات تحديد الهوية الشخصية التي بحوزتهم وإثبات الامتثال.
- يجب على مستخدمي أسيج الالتزام بهذه السياسة والإبلاغ عن أي حادث أمني أو عدم الالتزام بهذه السياسة إلى المدير التنفيذي للبيانات والأمن السيبراني / مالكي أصول البيانات / رئيس الإدارة.

1.5 الموافقة والتواصل والمراجعة

تتم الموافقة على سياسة خصوصية البيانات المحددة في هذه الوثيقة وفقا لعملية الموافقة على السياسة الخاصة ب ACIG. بعد الموافقة ، يجب نشرها وإبلاغها لجميع المستخدمين. يجب مراجعة مجموعة سياسة خصوصية البيانات سنويا أو في حالة حدوث تغييرات كبيرة لضمان استمرار ملاءمتها وكفايتها وفعاليتها.

1.6 ارتباط السياسات

اسم القسم	NCA-ECC	ISO 27001	GDPR	NDMO-NDGP	NIST
خصوصية البيانات والمعلومات	2-7-3-3	A.18.1.4	Article 5 to 46	Section 5	Appendix J

2. السياسة

2.1 بيانات السياسة العامة

• يجب على أسيج تحديد وتوثيق قوانين ولوائح الخصوصية المعمول بها. كما يجب على أسيج مراقبة أي تغييرات أو تحديثات تتعلق بقانون ولوائح الخصوصية المعمول بها لتعكس ذلك في سياسة الخصوصية والإشعار والممارسات الخاصة بها.

• ما لم يكن ذلك ضروريا لسبب وجيه في القانون السعودي ، يجب الحصول على موافقة صريحة من صاحب البيانات لجمع ومعالجة بياناته.

• يجب معالجة معلومات تحديد الهوية الشخصية بشكل قانوني وعادل وشفاف فيما يتعلق بموضوع البيانات.

• يجب تنفيذ وإنفاذ ضوابط وآليات خصوصية البيانات بما في ذلك الاسم المستعار والتشفير والإخفاء والترميز.

• يجب أن تكون آلية التحكم في خصوصية البيانات (بما في ذلك على سبيل المثال لا الحصر) ؛ حيث سيتم تقييم الاختيار الفني للحماية من قبل قسم البيانات والأمن السيبراني في ACIG.

2.2 مصادر معلومات تحديد الهوية الشخصية ACIG:

• مباشرة من صاحب البيانات بموافقته.

• غير مباشر ، ويجب على ACIG إبلاغ موضوع البيانات في غضون شهر واحد.

• يجب حماية معلومات تحديد الهوية الشخصية لأصحاب البيانات (أثناء تحديدها ونقلها ومعالجتها وإتلافها).

• يجب على ACIG تحديد وتوثيق واعتماد قائمة جرد معلومات تحديد الهوية الشخصية التي يتم جمع معلومات تحديد الهوية الشخصية واستخدامها ومعالجتها ومشاركتها ، (إذا لم يكن هناك غرض ، فلا ينبغي أن يكون هناك أي مجموعة لمعلومات تحديد الهوية الشخصية) التي توضح:

o فئة معلومات تحديد الهوية الشخصية المطلوبة

o احتياجات العمل والغرض (الأغراض) لكل فئة من فئات معلومات تحديد الهوية الشخصية

o وقت الاحتفاظ بمعلومات تحديد الهوية الشخصية

o المستلمون أو فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنها

o تفاصيل مصدر معلومات تحديد الهوية الشخصية إذا لم يتم جمع معلومات تحديد الهوية الشخصية من موضوع البيانات مباشرة ،

• يجب تخزين معلومات تحديد الهوية الشخصية لأصحاب البيانات أو معالجتها أو نقلها بطريقة دقيقة وكافية وذات صلة وتقتصر على ما هو ضروري ووفقا لاحتياجات العمل والاحتفاظ بمعلومات تحديد الهوية الشخصية التي تم تحديدها في موافقة صاحب البيانات وإشعار الخصوصية.

• لا يجوز استخدام معلومات تحديد الهوية الشخصية لأغراض الاختبار أو التدريب أو البحث.

• يجب مراجعة معلومات تحديد الهوية الشخصية لأصحاب البيانات وحذفها بانتظام بناء على احتياجات العمل أو الاحتفاظ بمعلومات تحديد الهوية الشخصية التي تم تحديدها في موافقة صاحب البيانات وإشعار الخصوصية.

• يجب إجراء تقييمات دورية لخصوصية البيانات لمعلومات تحديد الهوية الشخصية.

• يجب استضافة البيانات وفقا للوائح NCA لتكون داخل المملكة العربية السعودية. داخل خوادم ACIG ، أو الكيانات الأخرى ذات الصلة ب ACIG.

• يجب معالجة معلومات تحديد الهوية الشخصية المتعلقة بالإدانات والجرائم الجنائية أو التدابير الأمنية ذات الصلة فقط تحت سيطرة السلطة الرسمية.

• تقوم أسيج بتخزين ومعالجة معلومات تحديد الهوية الشخصية داخل المملكة العربية السعودية فقط وإنفاذ ذلك في عقود الطرف الثالث أو المستندات ذات الصلة، وعندما تحتاج أسيج إلى مشاركة معلومات تحديد الهوية الشخصية مع كيان آخر خارج المملكة، يجب أن تسعى للحصول على موافقة مكتب إدارة البيانات الوطنية.

2.3 حماية معلومات تحديد الهوية الشخصية

• يجب على أسيج ضمان السرية المستمرة لأنظمة وخدمات المعالجة وسلامتها وتوافرها ومرونتها.

• يجب على أسيج ضمان القدرة على استعادة توافر البيانات الشخصية والوصول إليها في الوقت المناسب في حالة وقوع حادث مادي أو فني.

• يجب على ACIG اختبار وتقييم وتقييم فعالية التدابير الفنية والتنظيمية بانتظام لضمان أمن المعالجة.

• يجب جمع معلومات تحديد الهوية الشخصية لأغراض محددة وصريحة ومشروعة ولا تتم معالجتها بطريقة لا تتوافق مع تلك الأغراض.

• يجب أن تكون معلومات تحديد الهوية الشخصية دقيقة ومناسبة ومحدثة. يجب اتخاذ خطوات معقولة لضمان مسح معلومات تحديد الهوية الشخصية غير الدقيقة المتعلقة بالأغراض أو تصحيحها دون تأخير.

• يجب الاحتفاظ بمعلومات تحديد الهوية الشخصية في شكل يسمح بتحديد موضوعات البيانات للوقت اللازم لأغراض معالجة معلومات تحديد الهوية الشخصية.

• يجب تنفيذ الضوابط الأمنية المناسبة لحماية معلومات تحديد الهوية الشخصية من المعالجة غير المصرح بها أو غير القانونية والخسارة أو التدمير أو التلف العرضي ، باستخدام التدابير الفنية أو التنظيمية المناسبة.

• إذا تم الحصول على معلومات تحديد الهوية الشخصية من مصادر أخرى غير موضوع البيانات ، فيجب إبلاغ موضوع البيانات ويجب إرسال إشعار خصوصية ACIG إليه أيضا.

2.4 حقوق صاحب البيانات

• عندما يمارس صاحب البيانات حقا بموجب قانون الخصوصية المعمول به، يجب على ACIG الرد باتخاذ أي إجراء يتطلبه قانون الخصوصية ذي الصلة، ما لم يكن من الواضح أن الطلب لا أساس له من الصحة أو مفرط. تتخذ أسيج الإجراء ذي الصلة في غضون شهر واحد من الاستلام ما لم يتم تحديد فترة مختلفة بموجب قانون الخصوصية المعمول به. هذا ينطبق على:

o الحق في الحصول على إذن منه / لها لجمع واستخدام وصيانة ومشاركة (PII) قبل جمعها ؛ أو قبل أي استخدامات جديدة أو الكشف عن معلومات تحديد الهوية الشخصية التي تم جمعها مسبقا.

- الحق في فهم عواقب قرارات الموافقة على أو رفض التصريح بجمع معلومات تحديد الهوية الشخصية واستخدامها ونشرها والاحتفاظ بها.
- الحق في سحب موافقته في أي وقت.
- الحق في الوصول أو الحصول على نسخة من معلومات تحديد الهوية الشخصية
- الحق في التصحيح
- الحق في المحو (الحق في النسيان)
- الحق في تقييد معالجة البيانات
- الحق في أن يتم إخطارك
- الحق في نقل البيانات
- الحق في الاعتراض
- الحق في الرد على شكاواه أو مخاوفه أو أسئلته.
- الحق في تقديم شكوى إلى سلطة إشرافية.
- الحق في الوصول إلى إشعار خصوصية أسيج.
- الحق في الوصول إلى جميع المعلومات في قائمة جرد معلومات تحديد الهوية الشخصية.

2.5 حقوق مالك البيانات

• يجب إبلاغ مالكي البيانات بحقوقهم ، بما في ذلك الحق في تقديم موافقة صريحة أو ضمنية على جمع بياناتهم الشخصية واستخدامها والكشف عنها.

• يجب أن يكون لدى مالكي البيانات خيارات متعددة لمنح أو حجب الموافقة على جمع بياناتهم الشخصية واستخدامها والكشف عنها.

• ينبغي أن تشمل خيارات الموافقة آليات الموافقة الصريحة والضمنية، مما يسمح لمالكي البيانات باختيار مستوى الموافقة الذي يناسب تفضيلاتهم وشواغلهم المتعلقة بالخصوصية.

• يجب أن تتضمن سجلات الموافقة تفاصيل الإشعار المقدم ، والخيارات المقدمة لمالكي البيانات ، والموافقة المحددة الممنوحة أو المرفوضة من قبل كل فرد.

• يجب منح مالكي البيانات الفرصة لمراجعة والتحقق من دقة واكتمال بياناتهم الشخصية قبل تقديم الموافقة.

2.6 الخصوصية حسب التصميم

• يجب أن تتبنى ACIG مبدأ الخصوصية حسب التصميم ويجب أن تضمن تلبية متطلبات الخصوصية في الأنظمة الحالية أو الجديدة أو المتغيرة بشكل كبير والتي تجمع أو تعالج معلومات تحديد الهوية الشخصية.

• يجب على ACIG إجراء تقييم لتأثير الخصوصية بانتظام على جميع الأنظمة التي تجمع أو تعالج معلومات تحديد الهوية الشخصية. ويشمل هذا التقييم ما يلي:

- تطبيق مبادئ حماية معلومات تحديد الهوية الشخصية

- o الوفاء بمسؤوليات المراقب المالي
- o تنفيذ ضوابط أمنية لحماية معلومات تحديد الهوية الشخصية
- o ضمان أن يكون الأساس القانوني لمعالجة معلومات تحديد الهوية الشخصية واضحا ولا لبس فيه
- o التأكد من أن جميع الموظفين المشاركين في التعامل مع معلومات تحديد الهوية الشخصية يفهمون مسؤولياتهم
- o ضمان جمع معلومات تحديد الهوية الشخصية أو استخدامها أو معالجتها أو تخزينها أو مشاركتها للغرض (الأغراض) المصرح به المحدد في إشعارات الخصوصية
- o التأكد من أن ACIG تقدم إشعارا فعالا للجمهور وموضوعات البيانات فيما يتعلق بأي تغييرات في أنشطتها تؤثر على الخصوصية ، بما في ذلك جمع معلومات تحديد الهوية الشخصية واستخدامها ومشاركتها وحمايتها وصيانتها والتخلص منها
- o اتباع القواعد المتعلقة بالموافقة
- o إجراء مراجعات منتظمة للإجراءات التي تنطوي على معلومات تحديد الهوية الشخصية
- o اعتماد الخصوصية حسب التصميم لجميع الأنظمة والعمليات الجديدة أو المتغيرة.

• يجب على ACIG تطبيق تقنيات مناسبة للأسماء المستعارة / إخفاء الهوية والتشفير لحماية معلومات تحديد الهوية الشخصية.

• يجب أن تفي ACIG بمتطلبات التوثيق التالية وتتيح الوصول إليها من قبل أصحاب البيانات فيما يتعلق بأنشطة المعالجة الخاصة بمعلومات تحديد الهوية الشخصية:

- o أغراض معالجة معلومات تحديد الهوية الشخصية
- o أنشطة المعالجة التي تتم على معلومات تحديد الهوية الشخصية
- o فئات معلومات تحديد الهوية الشخصية التي تمت معالجتها
- o اتفاقيات وآليات نقل معلومات تحديد الهوية الشخصية من وإلى المنظمات الأخرى بعد الحصول على موافقة أو طلب صاحب البيانات
- o جداول الاحتفاظ بمعلومات تحديد الهوية الشخصية
- o الضوابط الأمنية المعمول بها لحماية معلومات تحديد الهوية الشخصية

• يجب توعية موظفي أسيج بهذه السياسة ودورهم في حماية معلومات تحديد الهوية الشخصية.

2.7 الخصوصية بشكل افتراضي

• يجب على ACIG وضع التدابير الفنية والتنظيمية المناسبة لضمان عدم معالجة معلومات تحديد الهوية الشخصية بشكل افتراضي دون داع. ينطبق هذا على مقدار معلومات تحديد الهوية الشخصية التي تم جمعها ، ومدى معالجتها ، ومدة تخزينها ، ومن يمكنه الوصول إليها. يجب أن تضمن ACIG ، بشكل افتراضي ، عدم إتاحة معلومات تحديد الهوية الشخصية لعدد غير محدد من الأشخاص دون اتخاذ بعض الإجراءات من قبل موضوع البيانات.

2.8 نقل معلومات تحديد الهوية الشخصية

• يجب أن يستند أي نقل لمعلومات تحديد الهوية الشخصية إلى موافقة أو طلب صاحب البيانات.

• قبل نقل معلومات تحديد الهوية الشخصية خارج ACIG ، يجب تنفيذ تحليل تأثير الخصوصية.

• يجب إرسال إشعار مناسب إلى موضوع البيانات بما في ذلك المستلمين الذين سيتم نقل معلومات تحديد الهوية الشخصية إليهم ، بما في ذلك تاريخ وطبيعة وغرض كل إفصاح عن السجل ؛ وأسماء وعناوين المستلمين الذين تم الكشف عنهم.

• يجب تأكيد كفاية حماية معلومات تحديد الهوية الشخصية في الطرف المتلقي ؛ وهذا يشمل:

- o اسم المنظمة المتلقية والتفاصيل ذات الصلة
- o أغراض معالجة معلومات تحديد الهوية الشخصية
- o فئات الأفراد ومعلومات تحديد الهوية الشخصية التي تمت معالجتها
- o فئات متلقي معلومات تحديد الهوية الشخصية
- o اتفاقيات وآليات نقل معلومات تحديد الهوية الشخصية
- o جداول الاحتفاظ بمعلومات تحديد الهوية الشخصية
- o الضوابط الفنية والتنظيمية ذات الصلة المعمول بها

2.9 متطلبات الأطراف الثالثة

• يجب على ACIG إنشاء وتوثيق واعتماد متطلبات الخصوصية (الجمع والاستخدام والمعالجة والمشاركة) للمقاولين والمعالجين ومقدمي الخدمات ؛ وإدراجها في العقود والوثائق الأخرى ذات الصلة.

• عندما تشترك ACIG ووحدة تحكم أخرى في تحديد أغراض ووسائل المعالجة ، يجب أن يكونا مراقبين مشتركين. يجب عليهم بطريقة شفافة تحديد مسؤولياتهم عن الامتثال للالتزامات بموجب قوانين ولوائح الخصوصية المعمول بها.

• عندما تتم المعالجة نيابة عن ACIG ، يجب أن تستخدم فقط المعالجات التي توفر ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تفي المعالجة بمتطلبات قوانين ولوائح الخصوصية المعمول بها وتضمن حماية حقوق موضوع البيانات.

2.10 معالجة السجلات والمراقبة

• تقوم أسيج بتسجيل أنشطة المعالجة. ويجب أن يتضمن هذا السجل، على سبيل المثال لا الحصر، المعلومات التالية:

- o اسم وتفاصيل الاتصال بوحدة التحكم والمعالج
- o أغراض المعالجة
- o وصف لفئات أصحاب البيانات وفئات البيانات الشخصية

• تتيح المجموعة السجل لمراجع حسابات المنظمة والسلطة الإشرافية عند الطلب.

• يجب على ACIG مراجعة مخزون معلومات تحديد الهوية الشخصية بانتظام لضمان جمع معلومات تحديد الهوية الشخصية المحددة في الإشعار فقط والاحتفاظ بها ، وأن معلومات تحديد الهوية الشخصية لا تزال ضرورية لتحقيق الغرض المصرح به قانونا.

2.11 إشعار الخصوصية

• يجب على ACIG تحديد وتوثيق واعتماد وتنفيذ المتطلبات لتقديم إشعار فعال للجمهور وموضوعات البيانات فيما يتعلق بما يلي:

- o أنشطتها التي تؤثر على الخصوصية ، بما في ذلك جمع معلومات تحديد الهوية الشخصية واستخدامها ومشاركتها وحمايتها وصيانتها والتخلص منها
- o سلطة جمع معلومات تحديد الهوية الشخصية
- o الخيارات ، إن وجدت ، التي قد تكون لدى الأفراد فيما يتعلق بكيفية استخدام المنظمة لمعلومات تحديد الهوية الشخصية وعواقب ممارسة أو عدم ممارسة هذه الخيارات

o الحق في الوصول إلى معلومات تحديد الهوية الشخصية وتعديلها أو تصحيحها إذا لزم الأمر

o معلومات تحديد الهوية الشخصية التي تجمعها المنظمة والغرض (الأغراض) التي تجمع من أجلها تلك المعلومات

o كيف تستخدم المنظمة معلومات تحديد الهوية الشخصية

o ما إذا كانت المنظمة تشارك معلومات تحديد الهوية الشخصية مع الكيانات الخارجية ، وفئات تلك الكيانات ، وأغراض هذه المشاركة ؛

o ما إذا كان الأفراد لديهم القدرة على الموافقة على استخدامات محددة أو مشاركة معلومات تحديد الهوية الشخصية وكيفية ممارسة أي موافقة من هذا القبيل ؛

o كيف يمكن للأفراد الحصول على معلومات تحديد الهوية الشخصية أو الحصول عليها ؛

o كيف ستتم حماية معلومات تحديد الهوية الشخصية ؛

o الفترة التي سيتم تخزين معلومات تحديد الهوية الشخصية فيها

o وجود الحق في طلب الوصول إلى البيانات الشخصية وتصحيحها أو محوها أو تقييد المعالجة المتعلقة بموضوع البيانات أو الاعتراض على المعالجة وكذلك الحق في إمكانية نقل البيانات ؛

o وجود الحق في سحب الموافقة في أي وقت ،

o الحق في تقديم شكوى أو مخاوف أو أسئلة إلى ACIG وتقديم شكوى إلى سلطة إشرافية

o ما إذا كان توفير البيانات الشخصية مطلوبا قانونا ، أو شرطا ضروريا لإبرام عقد ، وكذلك ما إذا كان موضوع البيانات ملزما بتقديم البيانات الشخصية والعواقب المحتملة لعدم تقديم هذه البيانات

o التغييرات في الممارسات أو السياسات التي تؤثر على معلومات تحديد الهوية الشخصية أو التغييرات في أنشطتها التي تؤثر على الخصوصية ، قبل أو في أقرب وقت ممكن عمليا بعد التغيير.

• يجب على ACIG التأكد من أن ممارسات الخصوصية الخاصة بها متاحة للجمهور من خلال مواقع الويب التنظيمية.

• يجب على أسيج إبلاغ موضوع البيانات قبل رفع قيود المعالجة. إذا كانت المعالجة مقيدة من قبل موضوع البيانات ، فيجب معالجة البيانات الشخصية ، باستثناء التخزين ، فقط بموافقة موضوع البيانات.

• يجب على أسيج إبلاغ أي تصحيح أو محو للبيانات الشخصية أو تقييد المعالجة إلى كل مستلم تم الكشف عن البيانات الشخصية له. يجب على وحدة التحكم إبلاغ موضوع البيانات عن هؤلاء المستلمين إذا طلب موضوع البيانات ذلك.

• يجب على ACIG إبلاغ موضوع البيانات بالضمانات المناسبة للنقل حيث يتم نقل البيانات الشخصية إلى بلد ثالث أو إلى منظمة دولية.

• يجب على ACIG ضمان وصول الجمهور إلى المعلومات حول هوية المنظمة وتفاصيل الاتصال بها.

• يجب الإبلاغ عن خرق البيانات الشخصية ضمن الإطار الزمني المحدد في سياسة المكتب الوطني لإدارة البيانات بشأن حماية البيانات الشخصية ، وهو 72 ساعة من وقت اكتشاف الخرق.

• تضمن ACIG وصول الجمهور إلى المعلومات حول أنشطة الخصوصية الخاصة بها وقدرتها على التواصل مع مسؤول الخصوصية الخاص بها.

• يجب على ACIG التأكد من أن ممارسات الخصوصية الخاصة بها متاحة للجمهور من خلال مواقع الويب التنظيمية.

2.12 خرق الخصوصية

• يجب على ACIG تطوير وتوثيق واعتماد خطة الاستجابة لحوادث الخصوصية وتنفيذها عند الحاجة.

• ACIG إذا حدث خرق مع احتمال أن يؤدي إلى خطر على خصوصية أو حماية معلومات تحديد الهوية الشخصية ، فيجب على ACIG اتباع إجراءات خطة الاستجابة لحوادث الخصوصية إبلاغ قسم DCS في غضون 72 ساعة.

• يجب على ACIG تطوير وتوثيق واعتماد وتنفيذ إجراء لإبلاغ موضوع البيانات بخرق معلومات تحديد الهوية الشخصية دون تأخير.

2.13 التدريب والتوعية

• يجب على ACIG تطوير وتوثيق واعتماد وتنفيذ وتحديث برنامج تدريب وتوعية شامل بانتظام يهدف إلى ضمان فهم الموظفين لمسؤوليات وإجراءات الخصوصية ، مثل إدارة التدريب الأساسي على الخصوصية والتدريب المستهدف على الخصوصية القائم على الأدوار للموظفين المسؤولين عن معلومات تحديد الهوية الشخصية أو للأنشطة التي تنطوي على معلومات تحديد الهوية الشخصية.