State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

مذكرة استرشادية بشأن إدارة دورة حياة البيانات الشخصية

PDPPL-202502AN (A)

إدارة حماية خصوصية البيانات الشخصية

الوكالة الوطنية للأمن السيبراني

التاريخ: أكتوبر 2025

الإصدار: 0.1

التصنيف: عام

سجل الوثيقة

رقم الإصدار	الوصف	التاريخ
1.0	وثيقة منشورة – 1.0	**أكتوبر 2025**

الوثائق ذات الصلة (المبادئ التوجيهية)

مرجع الوثيقة	عنوان الوثيقة
PDPPL-02050201A	مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050213A	إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02040203A	نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون
PDPPL-02050205A	حقوق الأفراد - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050206A	تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050208A	حماية خصوصية البيانات الشخصية المتضمنة بالتصميم والمتضمنة افتراضياً - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050209A	مراقبي ومعالجي البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050212A	سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050215A	معالجة البيانات الشخصية ذات الطبيعة الخاصة- المبادئ التوجيهية للمخاطبين بأحكام القانون
PDPPL-02050217A	إخطارات اختراق البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

الوثائق ذات الصلة (أدوات ونماذج التقييم)

عنوان أداة ونموذج التقييم
تحليل تأثير حماية خصوصية البيانات DPIA - المبادئ التوجيهية للمخاطبين بأحكام القانون
أداة إدارة خصوصية الموردين (باللغة الإنجليزية)

إخلاء المسؤولية / الحقوق القانونية

أُعدت هذه المذكرة الاستشارية لصالح الجهات المخاطبة بأحكام القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية (يُشار إليه فيما بعد حيثما ورد بـ "القانون")، والتي تقوم بجمع ومعالجة البيانات الشخصية.

تُخلي إدارة حماية خصوصية البيانات الشخصية (يُشار إليها فيما بعد حيثما وردت بـ "الإدارة") بالوكالة الوطنية للأمن السيبراني (يُشار إليها فيما بعد حيثما وردت بـ "الوكالة") مسؤوليتها القانونية عن أي استخدام أو تفسير لهذه المذكرة الاستشارية، بما في ذلك، عدم تحمل الإدارة المسؤولية عن أي عواقب للقرارات أو الإجراءات التي تتخذها المؤسسة استناداً إليها، وتلتزم الجهة المعنية المسؤولية القانونية الكاملة بشأن أي من الممارسات التي تتعلق بحماية خصوصية البيانات الشخصية الخاصة بها، بما في ذلك على سبيل المثال لا الحصر، مراجعة وتحديث سياساتها وإجراءاتها بشكل دوري لضمان الالتزام المستمر بأحكام القانون. ويجوز لكل من يستخدم هذه المذكرة الاستشارية الرجوع إلى مستشار قانوني و/أو مهني للحصول على المشورة القانونية أو غيرها.

ويجب عند إعادة إنتاج هذه الوثيقة، سواء بشكل كلي أو جزئي وبصرف النظر عن وسيلة النسخ، الإشارة إلى الإدارة والوكالة كمصدر ومالك للوثيقة.

وتتطلب أي عملية إعادة إنتاج لهذه الوثيقة، لأي سبب أو غرض، الحصول على إذن خطي مُسبق من الإدارة. وتحتفظ الإدارة بالحق في تقييم مدى صلاحية وقابلية استخدام أي نسخة مكررة من هذه الوثيقة تم إنشائها لأي غرض عام.

ولا يجوز تفسير التفويض الصادر من الإدارة على أنه بمثابة مصادقة على النسخة المعاد إنتاجها، ويتحمل المطوّر المسؤولية الكاملة عن عدم الترويج أو إساءة عرض هذا التفويض بأي وسيلة إعلامية أو في أي مناقشات شخصية أو اجتماعية.

الأساس القانوني

بالاطلاع على القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، وحيث أن **إدارة حماية خصوصية البيانات الشخصية** (يُشار إليها فيما بعد حيثما وَرَدت بـ "**الإدارة**") منوط بها تنفيذ أحكام القانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية (يُشار إليه فيما بعد حيثما وَرَد بـ "**القانون**") والقرارات المُنفذة له باعتبارها الإدارة المختصة، وتتولى مباشرة كافة الاختصاصات والصلاحيات اللازمة بشأن التحقيق في الشكاوى المنطوية على وقائع تتعلق باختراق خصوصية البيانات الشخصية، بما في ذلك، اتخاذ ما يلزم من تدابير وقائية وتنظيمية بهذا الشأن.

وعليه، فقد نصت المادة (27) من أحكام القانون على أحقية الإدارة باتخاذ كافة التدابير اللازمة لتطبيق وتنفيذ أحكامه، كما نصت المادة (8/ بند 3) من ذات القانون على اختصاص الإدارة بتحديد الاحتياطات الإدارية والفنية والمادية المناسبة التي يجب على الجهة المخاطبة بأحكام القانون الالتزام بها لضمان امتثالها لأحكام القانون والقرارات الصادرة تنفيذاً له.

أُعدت هذه المذكرة الاستشارية مع الأخذ في الاعتبار القوانين والتشريعات السارية حاليًا في دولة قطر. وفي حال وجود أي تعارض بين هذه الوثيقة وأحكام القوانين القطرية، يُعتد بتلك القوانين والتشريعات، ويُستبعد أي نص يتعارض معها من هذه الوثيقة بالقدر اللازم، دون المساس بباقي أحكامها. وفي هذه الحالة، يجب إدخال التعديلات اللازمة لضمان التوافق مع القوانين والتشريعات المعمول بها في دولة قطر. وتنوه الإدارة بأن ما ورد من أحكام في هذه المذكرة الاستشارية ليست شاملة بشكل كامل، ويجب قراءتها بالاقتران مع أحكام القانون والقرارات الصادرة تنفيذاً له والمبادئ التوجيهية الصادرة عن الإدارة.

المذكرة الاستشارية تكمل المبادئ التوجيهية وتنوي المساهمة في تطبيق حدود الامتثال القانوني، وتقدم توصيات عملية وممارسات مُنظمة ومناهج حوكمة مهمة لتعزيز الامتثال، ودعم المساءلة، وترسيخ إدارة خصوصية البيانات الشخصية ضمن العمليات اليومية. وتشكل المبادئ التوجيهية والمذكرات الاستشارية معاً مجموعة شاملة من الأدوات التي ترسخ من خلالها ارشادات الامتثال لأحكام القانون، بينما تساهم المذكرة الاستشارية في تعزيز ثقافة إدارة المخاطر الاستباقية والمساءلة، مما يسهم في تحسين الموقف المؤسسي المتعلق بخصوصية البيانات الشخصية كما يشار اليه فيما بعد حيثما وردت بـ "**خصوصية البيانات**").

جدول المحتويات

1. المقدمة

تمثل إدارة البيانات الشخصية عملية مستمرة تمر بعدة مراحل، تبدأ من جمع البيانات ومعالجتها، ثم تخزينها، ومشاركتها، وأرشفتها، وانتهاءً بإتلافها. وتطرح كل مرحلة من مراحل دورة حياة البيانات الشخصية تحديات ومتطلبات امتثال خاصة بها، يتعيّن على الجهات المعنية التعامل معها لضمان المعالجة المسؤولة للبيانات الشخصية.

تُقدم هذه المذكرة الاستشارية إطار عمل منظم يعمل على توجيه المؤسسات بشأن إدارة البيانات الشخصية خلال مختلف مراحل دورة حياتها، بما يتوافق مع متطلبات أحكام القانون. كما تتضمن المذكرة أبرز الاعتبارات والممارسات الموصى بها لكل مرحلة، بما يمكّن المؤسسات من وضع ضوابط فعالة، والحد من المخاطر، وحماية حقوق الأفراد المتعلقة بخصوصية بياناتهم. وتسعى المذكرة إلى دعم المؤسسات في تحقيق الامتثال التنظيمي، وتعزيز ثقافة المساءلة والشفافية في إدارة البيانات الشخصية.

2. ما هي دورة حياة البيانات الشخصية؟

تشير دورة حياة البيانات الشخصية إلى سلسلة المراحل التي تمر بها البيانات الشخصية، بدءً من جمعها أو إنشائها وحتى إتلافها بصورة كاملة. وتفرض كل مرحلة من مراحل هذه الدورة مسؤوليات والتزامات محددة يتعيّن على المؤسسات الالتزام بها لضمان التعامل مع البيانات بطريقة قانونية وآمنة ومتوافقة مع المتطلبات التنظيمية.

وفيما يلي المراحل الرئيسية لدورة حياة البيانات الشخصية:

مرحلة دورة الحياة	التعريف
الجمع/الإنشاء	الحصول على البيانات الشخصية أو إنشاؤها لأغراض مشروعة.
الاستخدام	معالجة البيانات الشخصية لتلبية المتطلبات التشغيلية أو التحليلية أو القانونية.
المشاركة	نقل البيانات الشخصية مع تطبيق التدابير المناسبة بين فروع أو مكاتب المؤسسة خارج دولة قطر، أو إلى أطراف ثالثة داخل أو خارج دولة قطر.
التخزين	الاحتفاظ بالبيانات بشكل آمن لمدة محددة، مع ضمان سريتها وتوافرها وسلامتها.
الأرشفة	نقل البيانات إلى وحدة تخزين غير نشطة مع الحفاظ على إمكانية الوصول إليها لأغراض قانونية أو توثيقية.
الإتلاف	حذف البيانات الشخصية بشكل آمن أو تحويلها إلى صيغة غير معرّفة عند عدم الحاجة إليها.

3. فوائد إدارة دورة حياة البيانات الشخصية

تُعد الإدارة السليمة للبيانات الشخصية خلال دورة حياتها أمراً بالغ الأهمية لتمكين المؤسسات من الامتثال للمتطلبات التنظيمية لأحكام القانون، والحد من المخاطر المرتبطة باختراق البيانات أو الوصول غير المصرح به أو العقوبات المترتبة على عدم الامتثال، ويسهم تطبيق إطار عمل واضح لإدارة دورة حياة البيانات في تحقيق العديد من الفوائد، بما في ذلك ما يلي:

- **الامتثال التنظيمي**: يضمن هذا الإطار التوافق مع المتطلبات القانونية والتنظيمية من خلال تطبيق ضوابط منظمة عبر جميع مراحل دورة حياة البيانات الشخصية، مما يقلل من مخاطر فرض العقوبات أو اتخاذ الإجراءات القانونية.
- **أمن البيانات وخصوصيتها**: يحمي هذا الإطار البيانات الشخصية من الوصول غير المصرح به أو إساءة الاستخدام أو الاختراق، من خلال تطبيق تدابير تقنية وتنظيمية مناسبة، بما يضمن سرية البيانات وسلامتها وتوافرها طوال دورة حياتها.
- **الكفاءة التشغيلية**: يعمل هذا الإطار على تبسيط إجراءات التعامل مع البيانات، وتقليل التكرار، وتحسين الكفاءة، مع تسهيل الوصول السريع إلى البيانات عند الحاجة التشغيلية أو عند إجراء تدقيق الامتثال.
- **الحد من المخاطر**: يحدد هذا الإطار مخاطر خصوصية البيانات وأمنها المحتملة في كل مرحلة من مراحل دورة الحياة، ويطبق التدابير اللازمة للتخفيف منها.
- **تعزيز الثقة والعمليات التجارية**: يعزز هذا الإطار الثقة لدى أصحاب المصلحة من خلال إظهار ممارسات مسؤولة في إدارة البيانات.
- **المساءلة والشفافية**: يرسّخ هذا الإطار ممارسات التوثيق الواضحة وتسجيل أنشطة المعالجة، مما يعزز الشفافية مع الجهات الرقابية وأصحاب المصلحة، ويُسهم في بناء الثقة مع العملاء وأصحاب البيانات من خلال إثبات التزام الجهة بإدارة البيانات بشكل مسؤول.

ومن خلال تنفيذ إدارة فعّالة لدورة حياة البيانات الشخصية، تتمكن المؤسسات من حماية البيانات، ودعم الامتثال التنظيمي، وتحقيق أهدافها التجارية، مع ضمان خصوصية البيانات وأمنها.

4. اعتبارات الخصوصية عبر مراحل دورة حياة البيانات الشخصية

تتطلب الإدارة الفعالة للبيانات الشخصية مراعاة اعتبارات خصوصية البيانات محددة في كل مرحلة من مراحل دورة حياتها. ويجب على المؤسسات التأكد من أن البيانات الشخصية تُعالَج بطريقة قانونية وعادلة وشفافة، مع تطبيق التدابير المناسبة لتقليل المخاطر على حقوق الأفراد في خصوصية البيانات. وتتناول الفقرات التالية أبرز اعتبارات خصوصية البيانات (وفقاً لمتطلبات القانون وأفضل الممارسات الأخرى) في مختلف مراحل دورة حياة البيانات الشخصية، مع الإشارة إلى أهمية قيام المؤسسات بتقييم ما إذا كانت هناك اعتبارات إضافية أخرى تنطبق بحسب طبيعة أنشطة المعالجة، والعمليات التشغيلية، والمشهد التنظيمي السائد.

4.1 الجمع/الإنشاء

- **تحديد الغرض**: ينبغي على المؤسسات تحديد الأغراض المحددة التي يتم من أجلها جمع أو إنشاء البيانات الشخصية، على نحو يحقق التوافق مع الأهداف المؤسسية والمتطلبات التنظيمية. ويجب أن يكون جمع البيانات مبرراً وموثقاً بما يمنع الغموض بشأن الغرض من استخدامها.
- **الشفافية والإشعار**: يجب تزويد الأفراد بإشعارات خصوصية البيانات واضحة ومتكاملة في نقطة جمع البيانات، تتضمن أنواع البيانات التي يتم جمعها، والغرض من جمعها بما في ذلك الأساس القانوني، وفترات الاحتفاظ بها، وحقوقهم ذات الصلة.
- **إدارة الموافقات**: عندما يكون ذلك مناسباً، يجب الحصول على موافقة صريحة وموثقة من الأفراد. ويجب توفير آليات تتيح للأفراد سحب موافقتهم في أي وقت دون الإضرار بهم، وإذا لم تكن الموافقة هي الأساس القانوني المناسب للمعالجة، فيجب أن يتم جمع البيانات استناداً إلى غرض قانوني بديل.
- **تقليل البيانات**: يجب على المؤسسات التأكد من جمع الحد الأدنى من البيانات الشخصية اللازمة لتحقيق الغرض المحدد فقط.
- **الدقة**: عند جمع البيانات الشخصية، قد يُلزم على الجهات المعنية التحقق من دقة البيانات المُجمعة، كما يجب إجراء مراجعات دورية للتحقق من دقة البيانات وملاءمتها.
- **التعامل مع البيانات ذات الطبيعة الخاصة**: يجب تطبيق تدابير إضافية عند جمع البيانات الشخصية ذات الطبيعة الخاصة. كما يجب على المؤسسات الحصول على إذن من الإدارة قبل معالجة هذه البيانات، وضمان الامتثال للمتطلبات المعمول بها.

- **تدابير الأمن**: يجب تطبيق تدابير تقنية وتنظيمية كافية، مثل التشفير وبروتوكولات النقل الآمن، لحماية البيانات أثناء عملية الجمع.
- **التوثيق**: يجب توثيق أنشطة الجمع ضمن سجل معالجة البيانات الشخصية، متضمناً فئات البيانات، ومصادرها، والأسس القانونية المعتمدة. ويجب مراجعة وتحديث السجل بشكل دوري.

المراجع:

مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

معالجة البيانات الشخصية ذات الطبيعة الخاصة- المبادئ التوجيهية للمخاطبين بأحكام القانون

نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

4.2 الاستخدام

- **تقييد الغرض**: يجب استخدام البيانات الشخصية فقط للأغراض المحددة التي جُمعت من أجلها، كما هو موضح في إشعار خصوصية البيانات. ويجب تجنب إعادة استخدام البيانات أو توسيع أنشطة المعالجة بطريقة غير مصرح بها.
- **التغييرات في استخدام البيانات الشخصية**: في حال حدوث تغييرات في كيفية استخدام البيانات الشخصية، يجب إجراء تقييم تحليل تأثير حماية خصوصية البيانات لتقييم المخاطر المحتملة. كما يجب إخطار الأفراد من خلال إشعار خصوصية البيانات، والحصول على موافقتهم، أو تحديد غرض قانوني سليم قبل الشروع في تنفيذ التغييرات. وإذا شملت التغييرات بيانات ذات طبيعة خاصة، يتعين على المؤسسات إخطار الإدارة للتحقق من صحة التصريح القائم وضمان الاستمرار في الامتثال لأحكام القانون.
- **ضوابط الوصول**: يجب تقييد الوصول إلى البيانات الشخصية على الموظفين المخولين فقط، وفق مبدأ الحاجة للمعرفة، باستخدام آليات قوية للتحكم في الوصول، مع إجراء مراجعات دورية لصلاحيات الوصول.
- **جودة البيانات ودقتها**: يجب وضع آليات لضمان دقة البيانات وتحديثها بشكل مستمر أثناء استخدامها، مع منح الأفراد الفرصة لطلب تصحيح أية معلومات غير دقيقة.

- **التدابير الأمنية**: يجب تطبيق تدابير تقنية وتنظيمية مناسبة، مثل التشفير، وإخفاء الهوية الجزئي، وبرامج التوعية، وأنظمة الرصد، لحماية البيانات من الاستخدام غير المصرح به أو التسريب أو الاختراق أثناء المعالجة.
- **التدقيق والمراقبة**: يجب تنفيذ عمليات تدقيق ومراقبة دورية للتأكد من استخدام البيانات بما يتوافق مع المتطلبات القانونية والسياسات المؤسسية المعتمدة.
- **إدارة اختراقات البيانات الشخصية**: يجب على المؤسسة إعداد خطة أو برنامج لإدارة اختراقات البيانات الشخصية، يشمل تحديد الاختراق، والإبلاغ في الوقت المناسب عن تفاصيله إلى أصحاب المصلحة المعنيين، بما في ذلك الإدارة والأفراد المتضررين.

المراجع:

مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

أداة تحليل تأثير حماية خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

إخطارات اختراق البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

حقوق الأفراد - المبادئ التوجيهية للمخاطبين بأحكام القانون

4.3 المشاركة

- **العناية الواجبة**: قبل مشاركة البيانات الشخصية، يجب على المؤسسات تقييم مدى امتثال الجهات المعالجة من الأطراف الثالثة للوائح حماية البيانات ومعايير الأمن المعتمدة.
- **تقييد الإفصاح**: يجب على المؤسسات حصر مشاركة البيانات الشخصية في الحدود اللازمة لتحقيق الغرض المقصود، مع تنفيذ ضوابط مناسبة لمنع الإفصاح غير المصرح به أو المفرط.
- **اتفاقيات معالجة البيانات**: يجب إبرام اتفاقيات قانونية ملزمة مع الأطراف الثالثة، تُحدَّد فيها المسؤوليات والمتطلبات الأمنية والتزامات الإبلاغ عن الاختراقات.
- **متطلبات نقل البيانات عبر الحدود**: يجب على المؤسسات التأكد من أن الجهة المستقبلة للبيانات توفر – على الأقل – مستوى الحماية المنصوص عليه في القانون، وذلك من خلال الوسائل التعاقدية.

- **التقييم الدوري للأطراف الثالثة**: يجب مراجعة الجوانب المتعلقة بخصوصية البيانات وأمنها لدى الجهات المعالجة من الأطراف الثالثة بشكل دوري لضمان استمرار الامتثال لمتطلبات قانون حماية خصوصية البيانات الشخصية.
- **التغييرات في ممارسات مشاركة البيانات**: يجب تقييم أي تغييرات في ممارسات مشاركة البيانات من حيث توافقها مع قانون حماية خصوصية البيانات الشخصية، وتحديث العقود والسجلات لتعكس هذه التغييرات.
- **الشفافية مع الأفراد**: يجب إبلاغ الأفراد بأي ممارسات لمشاركة البيانات، بما في ذلك الغرض وفئات الجهات المستلمة، من خلال إشعارات خصوصية البيانات محدثة.
- **التوثيق**: يجب الاحتفاظ بسجل شامل للجهات المعالجة للبيانات، على أن يُراجَع ويُحدَّث بانتظام لضمان الامتثال المستمر.

المراجع:

مراقبي ومعالجي البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

أداة إدارة خصوصية الموردين

إشعار الخصوصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

4.4 التخزين

- **مدة الاحتفاظ**: يجب على المؤسسات تحديد مدد الاحتفاظ بالبيانات الشخصية بما يتوافق مع المتطلبات القانونية والتنظيمية والتشغيلية.
- **سياسات الاحتفاظ**: يتعين على المؤسسات تطبيق سياسات الاحتفاظ على الأنظمة ومستودعات البيانات لضمان الاحتفاظ بالبيانات الشخصية وفقاً للمدد المحددة.
- **التخزين الآمن**: يجب حماية البيانات المخزنة من خلال تدابير أمنية مناسبة مثل التشفير، وضوابط الوصول الآمن، وحلول النسخ الاحتياطي، لمنع الوصول غير المصرح به البيانات أو فقدانها أو اختراقها.
- **المراجعة والتنظيف الدوري**: يجب إجراء مراجعات دورية للبيانات المخزنة لتحديد المعلومات القديمة أو الزائدة عن الحاجة وإزالتها.

- **توثيق التخزين**: يجب توثيق مواقع وأساليب التخزين ضمن سجل أنشطة المعالجة لضمان تتبع البيانات والامتثال لسياسات التخزين.

المراجع:

مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

سجل معالجة البيانات الشخصية - المبادئ التوجيهية للمخاطبين بأحكام القانون

نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

4.5 الأرشفة

- **ممارسات أرشفة البيانات المشروعة**: يجب على المؤسسات أرشفة البيانات لأغراض مشروعة فقط، مثل الامتثال أو التدقيق أو التحليل التاريخي، مع توفر مبررات قانونية لاستمرار الاحتفاظ بها.
- **قيود الوصول**: يجب إخضاع البيانات المؤرشفة لضوابط وصول صارمة للحد من الاسترجاع غير المصرح به.
- **المراجعات الدورية**: يجب تقييم البيانات المؤرشفة بشكل دوري لضمان استمرار ملاءمتها وامتثالها لمتطلبات الاحتفاظ.
- **التدابير الأمنية**: يجب تطبيق تدابير أمنية مادية ورقمية، مثل التشفير والتخزين الآمن، لحماية البيانات المؤرشفة.

المراجع:

مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

4.6 الإتلاف

- **أساليب الإتلاف الآمن**: يجب حذف البيانات الشخصية التي لم تعد مطلوبة باستخدام أساليب إتلاف معتمدة ومعترف بها في القطاع لضمان عدم إمكانية استعادتها.
- **التوثيق والمساءلة**: يجب الاحتفاظ بسجل للإتلاف، يتضمن تفاصيل البيانات التي تم حذفها، وتاريخ الإتلاف، والجهة أو الشخص الذي قام بذلك، لإثبات الامتثال.

- **إلغاء الهوية كحل بديل**: في الحالات التي يتعذر فيها الحذف، ينبغي النظر في تطبيق تقنيات إلغاء الهوية لمنع إمكانية إعادة التعرف على البيانات مع الحفاظ على قيمتها.

من خلال اعتماد نهج منظم ومبدئي لإدارة دورة حياة البيانات الشخصية، يمكن للمؤسسات تحقيق الامتثال لأحكام القانون، وحماية خصوصية البيانات، وحماية حقوق الأفراد. وتُسهم هذه المذكرة الاستشارية في ترسيخ مبدأ المساءلة، وتقليل المخاطر، وتعزيز الثقة مع أصحاب المصلحة.

المراجع:

مبادئ خصوصية البيانات - المبادئ التوجيهية للمخاطبين بأحكام القانون

نظام إدارة حماية البيانات الشخصية - قائمة المراجعة للمخاطبين بأحكام القانون

نهاية الوثيقة