SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

الدليل الاسترشادي لإتلاف البيانات الشخصية وإخفاء الهوية والترميز

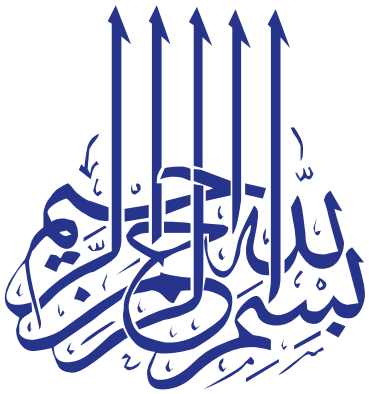
تصنيف الوثيقة: عام

رقم الإصدار ١.٠

أغسطس ٢٠٢٤

تنويه

لا يغني الدليل الاسترشادي عن الرجوع إلى نظام حماية البيانات الشخصية ولوائحه التنفيذية والقواعد والقرارات ذوات الصلة لضمان الالتزام بأحكام النظام واللوائح.


بسم الله الرحمن الرحيم

قائمة المحتويات

المقدمة ٥
الهدف ٥
اولاً: إتلاف البيانات الشخصية ٦
ثانياً: إخفاء الهوية ٧
ثالثاً: الترميز ٨
رابعاً: إرشادات عامة ٩

المقدمة

نظراً للدور الذي تضطلع به الهيئة السعودية للبيانات والذكاء الاصطناعي في رفع مستوى الوعي لدى الجهات المشمولة بأحكام نظام حماية البيانات الشخصية "النظام" ولوائحه التنفيذية ولتمكينهم من معرفة التزاماتهم الواردة في المادة (الثامنة عشرة) من النظام، وما ورد في شأنه في المادة (الثامنة) والمادة (التاسعة) من اللائحة التنفيذية، أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي هذا الدليل الاسترشادي بغرض مساعدة الجهات في تحديد الحالات التي يجب فيها إتلاف البيانات الشخصية أو إخفاء هوية أصحابها.

كما يقدم هذا الدليل بعض الأمثلة على التقنيات المساعدة في الإتلاف وإخفاء الهوية والترميز. ويمكن الرجوع إلى النظام ولوائحه التنفيذية لتحديد المقصود بالألفاظ والعبارات الواردة في هذا الدليل، وتحديد المتطلبات النظامية، فلا يمكن أن يُغني الاطلاع على هذا الدليل عن الرجوع إلى أحكام النظام ولوائحه التنفيذية، ولا يعد هذا الدليل نصاً نظامياً ملزماً؛ إذ تمثل أحكام النظام ولوائحه التنفيذية المرجعية النظامية لجميع ما يتعلق بتطبيق أحكامه.

الهدف

يهدف هذا الدليل إلى الآتي:

١- دعم الجهات في تطبيق أحكام النظام.

٢- تشجيع الجهات على تبني أفضل ممارسات إتلاف البيانات الشخصية وإخفاء الهوية والترميز.

٣- تقديم بعض الأمثلة التقنية لجهات التحكم لمساعدتها في تطبيق أحكام إتلاف البيانات الشخصية وإخفاء الهوية والترميز الواردة في النظام ولوائحه التنفيذية.

٤- المساهمة في تمكين أصحاب البيانات الشخصية من ممارسة حقوقهم المنصوص عليها في النظام.

٥- المحافظة على خصوصية أصحاب البيانات الشخصية.

اولاً: إتلاف البيانات الشخصية

في الحالات التي يجب على جهة التحكم إتلاف البيانات الشـخصـية، التأكد من ضـمان إتلافها بشـكل نهائي يجعل من المتعذر الاطلاع عليها أو اسـتعادتها مرة أخرى أو معرفة صـاحبها على وجه التحديد، كما أن عملية أرشـفة البيانات الشـخصـية والنسـخ الاحتياطي لا تعد من قبيل عمليات الإتلاف ويجب التعامل معها كبيانات شـخصـية وفقاً لأحكام النظام ولوائحه، ومع مراعاة مانصـت عليه المادة (الثامنة عشـرة) من النظام والمتطلبات النظامية الأخرى المتعلقة بالإتلاف عموماً؛ حيث لا يغني هذا الدليل من التزام الجهات بالضـوابط والمعايير والقواعد ذوات الصـلة الصـادرة عن الهيئة الوطنية للأمن السـيبراني مثلاً، وغيرها من المتطلبات النظامية التي تقرها الجهات المختصة ذوات العلاقة.

١- **أحوال الإتلاف:** على جهة التحكم إتلاف البيانات الشخصية في أي من الأحوال الآتية:

أ- تنفيذاً لطلب صاحب البيانات الشخصية.

ب- إذا لم تعد البيانات الشخصية ضرورية لتحقيق الغرض الذي جمعت من أجله.

ج- إذا عدَل صـاحب البيانات الشـخصـية عن موافقته على جمع بياناته الشـخصـية، وكانت الموافقة هي المسوغ النظامي الوحيد للمعالجة.

د- إذا علمتْ أن البيانات الشخصية تجرى معالجتها بطريقة مخالفة للنظام.

٢- **شروط الإتلاف:** على جهة التحكم عند إتلافها للبيانات الشخصية القيام بالآتي:

أ- اتخاذ الإجراءات الملائمة لإشـعار الجهات الأخرى التي أفصـحت لها جهة التحكم عن البيانات الشخصية ذوات الصلة، وطلب إتلافها.

ب- اتخاذ الإجراءات الملائمة لإشـعار الأشـخاص الذين تم الإفصـاح لهم عن البيانات الشخصية بأي وسيلة كانت وطلب إتلافها.

ج- إتلاف كافة النسـخ المتعلقة بالبيانات الشـخصـية المخزنة في أنظمة جهة التحكم، بما في ذلك النسـخ الاحتياطية، على أن تراعي المتطلبات النظامية ذوات العلاقة بهذا الشأن.

٣- **أمثلة الإتلاف**

أ- **الكتابة على البيانات والمحو الآمن (SE):** الكتابة على البيانات وتتمثل في استبدال البيانات الأصلية ببيانات عشوائية لا معنى لها؛ مما يجعل البيانات الأصلية غير قابلة للاسترداد. يعد المحو الآمن تقنية أكثر تقدماً من الكتابة على البيانات، فهو يتضمن إرسال أمر إلى البرنامج المثبت بالجهاز لمحو جميع البيانات، بما في ذلك المناطق التي لا يمكن الوصول إليها في العادة.

ب- **إزالة البيانات (بدون إتلاف الأجهزة):** وتمثل هذه الطريقة استخدام مزيل التمغنط أو ما يسمى بـ (ديجاوسر) لتعطيل المجال المغناطيسي، الذي يخزن البيانات؛ مما يجعل البيانات غير قابلة للقراءة بشكل فعال. وتتميز هذه العملية بالكفاءة والسرعة؛ مما يجعلها الخيار المفضل لمحو البيانات المجمعة، كما أنها تبقي الجهاز سليماً لإعادة استخدامه. تعمل تقنية الإزالة (ديجاوسر) على الوسائط المغناطيسية فقط، وهي غير مناسبة لمحركات الأقراص ذات الحالة الصلبة (SSD) أو وحدات التخزين القائمة على استخدام الفلاش.

ج- **الطحن والتشويه:** تقطيع الأصول إلى أجزاء صغيرة؛ وتشويهها مادياً؛ مما يجعل الأصول غير قابلة للقراءة بشكل فعال.

ثانياً: إخفاء الهوية

على جهة التحكم التأكد من إزالة المعرفات المباشرة وغير المباشرة لصاحب البيانات الشخصية بطريقة تجعل من المتعذر تحديد هوية صاحبها، كما لا تعد البيانات التي جرى إخفاء هوية أصحابها بيانات شخصية، وبالتالي لا تخضع لنطاق نظام حماية البيانات الشخصية.

على جهة التحكم عند إخفائها لهوية صاحب البيانات الشخصية القيام بالآتي:

أ- التأكد من عدم إمكانية إعادة التعرف على هوية صاحب البيانات الشخصية بعد إخفاء هويته.

ب- تقويم الأثر بما في ذلك إمكانية إعادة تحديد هوية صاحب البيانات الشخصية، وذلك في الأحوال المنصوص عليها في الفقرة (١) من المادة (الخامسة والعشرون) من اللائحة التنفيذية.

ج- اتخاذ التدابير التنظيمية والإدارية والتقنية اللازمة لتجنب المخاطر، مع مراعاة التطورات التقنية وأساليب إخفاء الهوية وتحديثها ومواءمتها مع تلك التطورات.

د- تقويم فعالية تقنيات إخفاء هوية صاحب البيانات الشخصية المُطبقة، وإجراء التعديلات اللازمة لضمان عدم إمكانية إعادة التعرف على هوية صاحب البيانات الشخصية.

ثالثاً: الترميز

يعرف الترميز بأنه تحويل المعرفات الرئيسية التي تدل على هوية صاحب البيانات الشخصية إلى رموز تجعل من المتعذر تحديد هوية صاحب البيانات الشخصية بشكل مباشر دون استخدام بيانات أو معلومات إضافية، وأن يتم الاحتفاظ بتلك البيانات أو المعلومات الإضافية بشكل منفصل ووضع الضوابط الفنية والإدارية اللازمة لضمان عدم ربطها بصاحب البيانات الشخصية بشكل محدد.

تعد البيانات المرمزة بيانات شخصية، وذلك بسبب إمكانية تحديد هوية صاحب البيانات الشخصية بطريقة أو بأخرى، ويهدف استخدام اسلوب "الترميز" إلى الحفاظ على أمن البيانات الشخصية، ويستخدم كأحد التدابير التقنية المناسبة لتقليل المخاطر المتعلقة بمعالجة البيانات الشخصية للأفراد، إلا أنه لا يصل إلى مستوى درجة الحماية الذي يوفره إجراء "إخفاء الهوية". ومن الأمثلة على الترميز استبدال واحد أو أكثر من المعرفات التي تدل على هوية الفرد، مثال استبدال الاسم إلى رمز (كرقم مرجعي).

يتم استخدام الترميز عند الإفصاح عن بيانات شخصية تتضمن بيانات شخصية لفرد آخر غير صاحبها، فإنه يتم ترميز بيانات الفرد الآخر لضمان خصوصيته. أو في حال جمع البيانات الشخصية أو معالجتها لأغراض علمية أو بحثية أو إحصائية دون موافقة صاحبها وفي الأحوال التي لا يؤثر ذلك على تحقيق الغرض من المعالجة.

أمثلة على تقنيات إخفاء الهوية والترميز

يمكن أن تشمل التدابير التقنية على عدة أساليب حسب تنظيمات جهة التحكم والبيانات الشخصية محل المعالجة. كما يجب مراجعة هذه التقنيات وتحديثها بانتظام لضمان عدم ربطها بصاحب البيانات الشخصية بشكل محدد.

فيما يلي أمثلة على التقنيات المستخدمة:

أ- **التعميم (Generalization) :** اســتبدال ســمات محددة بقيم أكثر عمومية. على ســبيل المثال: تجميع الأعمار إلى فئات عمرية (٢٠-٣٠، ٣٠-٤٠) بدلا ً من اســتخدام الأعمار المحددة.

ب- **تجميع البيانات (Data Aggregation):** جمع البيانات الفردية في نطاق أو مجموعة أو فئة، على ســبيل المثال: تحديد ســنة الميلاد بدلاً من تاريخ الميلاد الكامل، ويتم التأكد من عدم إمكانية اســتخدام البيانات المجمعة لاســتنتاج معلومات حول أفراد معينين.

ج- **التشفير:** تشفير البيانات الشخصية باستخدام خوارزميات تشفير قوية، ويتم التأكد من تخزين مفاتيح التشفير بشكل آمن ومنفصل عن البيانات المشفرة.

د- **الإخفاء:** تطبيق تقنيات إخفاء البيانات لإخفاء أو حجب عناصر بيانات معينة.

رابعاً: إرشادات عامة

١- التأكد من أن جميع أنشــطة إخفاء الهوية والإتلاف والترميز تتوافق مع متطلبات نظام حماية البيانات الشــخصــية ولوائحه التنفيذية والمتطلبات النظامية التي تقرها الجهات المختصة ذوات العلاقة.

٢- توعية جميع الموظفين المشاركين في أمن البيانات بأهمية ترميز البيانات وإخفاء الهوية بشكل آمن.

٣- على جهة التحكم أن ألا تُفقد أي بيانات شـخصـية أو توضـع في غير مكانها أو يكُشـف عنها لأطراف خارجية غير مصرح لها أثناء عملية الإتلاف أو إخفاء الهوية أو الترميز.

٤- إتلاف جميع المســتندات المطبوعة بطريقة لا يمكن معها إعادة تكوين البيانات الشــخصــية أو اســتردادها (على ســبيل المثال: يجب أن يتضــمن تمزيق المســتندات المطبوعة اســتخدام آلات تمزيق آمنة والتخلص الآمن من النفايات) وفق المتطلبات النظامية التي تقرها الجهات المختصة ذوات العلاقة.

٥- الاحتفاظ بوثائق مفصـــلة لعمليات إخفاء الهوية والإتلاف، بما في ذلك التقنيات المستخدمة والأساس المنطقي لاختيارها، والتأكد من توفر الوثائق عند طلبها من قبل الجهة المختصة.

٦- على جهة التحكم مراجعة وتحديث تقنيات الإتلاف وإخفاء الهوية والترميز بشكل منتظم لمعالجة المخاطر الجديدة والتقدم التكنولوجي.

SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority