SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

الدليل الإجرائي لمعالجة حوادث تسرب البيانات الشخصية

تصنيف الوثيقة: عام

رقم الإصدار 1.0

أكتوبر 2024


بسم الله الرحمن الرحيم

قائمة المحتويات

المقدمة

انطلاقاً من دور الهيئة السعودية للبيانات والذكاء الاصطناعي (الهيئة) في دعم جهات التحكم بالالتزام بأحكام نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ المعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، ولوائحه التنفيذية، والتي تضمنت إلزام جهة التحكم بإشعار الهيئة عند علمها بحدوث تسرب لبيانات شخصية في الأحوال التي بينتها اللائحة، إضافة إلى إشعار صاحب البيانات الشخصية في حال ترتب على هذه الحادثة ضرر على بياناته أو تعارض مع حقوقه أو مصالحه، قامت الهيئة بإعداد هذا الدليل لتحديد الإجراءات اللازمة للتعامل مع حوادث تسرب البيانات الشخصية وتقليل الآثار والمخاطر المترتبة على أصحابها وفقا للنظام واللوائح التنفيذية.

التعريفات

تكون للألفاظ والعبارات الواردة في هذا الدليل المعاني الموضحة أمام كل منها في التعريفات الواردة في نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ ١٤٤٣/٢/٩هـ، والمعدل بموجب المرسوم الملكي رقم (م/148) وتاريخ ١٤٤٤/٩/٥هـ ولوائحه التنفيذية، ويُقصد بالألفاظ والعبارات الآتية -أينما وردت في هذا الدليل- المعاني الموضحة أمام كل منها، ما لم يقتضِ سياق النص خلاف ذلك:

#	المصطلح	التعريف
1	الدليل	الدليل الإجرائي لمعالجة حوادث تسرب البيانات الشخصية.
2	الهيئة	الهيئة السعودية للبيانات والذكاء الاصطناعي.
3	مسؤول حماية البيانات الشخصية	شخص طبيعي أو أكثر يتم تعيينه أو تحديده من قبل جهة التحكم يتولى متابعة تنفيذ جهة التحكم لأحكام النظام ولوائحه التنفيذية، ومراقبة الإجراءات المعمول بها داخل جهة التحكم والإشراف عليها، وتلقي الطلبات المتعلقة بالبيانات الشخصية وفقاً لأحكام النظام ولوائحه التنفيذية.

النطاق

يطبق هذا الدليل على جميع جهات التحكم المشـــمولة بتطبيق أحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية.

مراحل معالجة حوادث تسرب البيانات الشخصية:

المرحلة الأولى: إشعار الهيئة

دون الإخلال بتقديم أي بلاغ أو إشعار تسرب بيانات بموجب ما يصدر عن الهيئة الوطنية للأمن الســـيبراني أو أي أنظمة ولوائح معمول بها في المملكة، على جهة التحكم أن تُشـــعر الهيئة خلال مدة لا تتجاوز (72) ساعة من وقت علمها بالحادثة، إذا كان من شأن تلك الحادثة الإضرار بالبيانات الشخصية أو صاحب البيانات الشخصية أو كانت تتعارض مع حقوقه أو مصالحه عبر خدمة إشعار تسرب بيانات شخصية التي تقدمها الهيئة عبر منصة حوكمة البيانات الوطنية. حيث يستوجب التسجيل في المنصة للاستفادة من هذه الخدمة. على أن يتضمن الإشعار الآتي:

1. وصف لحادثة تسرب البيانات الشخصية، على أن يتضمن وقتها وتاريخها وكيفية وقوعها ووقت علم جهة التحكم بها.
2. الفئات والاعداد الفعلية او التقريبية لأصحاب البيانات الشخصية المعنيين، ونوع البيانات الشخصية.
3. وصف للمخاطر التي قد تنتج عن الحادثة، بما في ذلك مستوى الاثر الفعلي او المحتمل الذي قد يلحق بالبيانات الشخصية واصحاب البيانات الشخصية، والاجراءات والتدابير التي تم اتخاذها من قبل جهة التحكم للمنع او الحد من آثار تلك المخاطر وتخفيفها، والتدابير المستقبلية التي ستتخذها جهة التحكم لمنع تكرار الحادثة.
4. بيان إذا تم او سيتم اشعار صاحب البيانات الشخصية بتسرب بياناته الشخصية، وفقاً للمتطلبات المذكورة في المرحلة الثانية من هذا الدليل.

5. بيانات التواصل لجهة التحكم او مسؤول حماية البيانات الشخصية لديها – إن وجد – او اي مسؤول اخر تتوافر لديه معلومات فيما يخص الحادثة محل الاشعار.

تنويه: على جهة المعالجة وأي جهات أخرى وفقاً للتعاقدات اللاحقة اســـتناداً إلى المادة الثامنة من النظام، اتباع متطلبات الإشعار أعلاه بالتنسيق المباشر مع جهة التحكم.

المرحلة الثانية: احتواء حادثة التسرب

قيام جهة التحكم بالعمل على تطبيق إجراءات الاســـتجابة واحتواء حوادث تســـرب البيانات الشـخصـية؛ وفقاً لأفضـل الممارسـات العالمية والمتطلبات التنظيمية ذات العلاقة. ومنها على سبيل المثال لا الحصر الإجراءات الآتية لاحتواء حوادث تسرب البيانات الشخصية:

1. تحديد نوع وحجم البيانات الشخصية.
2. تحديد نوعية البيانات الشـخصـية المسـربة والقابلة للتغيير (مثل البريد الالكتروني، كلمة المرور، الأسـئلة السـرية، أرقام البطاقات الائتمانية، إلخ)، والعمل على تغيير تلك البيانات المسربة.
3. تحديد الأفراد المتضررين من حادثة التسرب، بناءً على نوعية البيانات الشخصية المسربة.
4. على جهة التحكم اشعار صاحب البيانات الشخصية دون تأخير غير مبرر؛ إذا كان يترتب على ذلك ضرر على بياناته أو تعارض مع حقوقه أو مصالحه، ومنها على سبيل المثال لا الحصر: أضـرار تتعلق بممارسـة حقوق صـاحب البيانات الشـخصـية، أضـرار جسـدية كالملاحقة، أو الاعتداء، أو أضرار اقتصادية كالاحتيال ،أو انتحال الشخصية.

أ. وسائل إشعار صاحب البيانات الشخصية:

1. يمكن لجهة التحكم إشـعار صـاحب البيانات الشـخصـية بأي وسـيلة مناسـبة وفقاً للوسـائل التي تم تفضيلها للتواصل من قبل صاحب البيانات الشخصية؛ ومنها على سبيل المثال لا الحصر، الرسائل النصية أو البريد الإلكتروني.

2. في حال اتساع ضرر التسرب لمجموعة كبيرة من الأشخاص على المستوى الوطني يمكن لجهة التحكم –على أن يتم مراعاة محتوى الإشعار وفقاً للمتطلبات النظامية المعمول بها في المملكة - بالإضافة الى ما ورد في الفقرة (1) أعلاه، إشعار اصحاب البيانات الشخصية بوسائل أخرى؛ ومنها على سبيل المثال لا الحصر، الموقع الإلكتروني الخاص بجهة التحكم، حسابات جهة التحكم الرسمية على منصات التواصل الاجتماعي، أو وسائل الإعلام.

ب. وصف الإشعار المقدم إلى صاحب البيانات الشخصية:

يكون الإشعار المقدم إلى صاحب البيانات الشخصية بلغة واضحة ومبسطة، ويتضمن الآتي:

1. وصف لحادثة تسرب البيانات الشخصية.
2. وصف المخاطر المحتملة الناشئة عن تسرب بياناته الشخصية والتدابير المتخذة لمنع تلك المخاطر او الحد منها وتخفيف اثارها.
3. اسم وبيانات التواصل لجهة التحكم ومسؤول حماية البيانات الشخصية لديها – إن وجد – أو اي وسائل تواصل اخرى مناسبة مع جهة التحكم.
4. تقديم التوصيات والنصائح اللازمة التي قد تساعد صاحب البيانات الشخصية المتضرر على اتخاذ الاجراءات الملائمة لتجنب المخاطر المحددة او تخفيف اثارها مثل أضرار اقتصادية كالاحتيال أو انتحال الشخصية.

المرحلة الثالثة: التوثيق

على جهة التحكم الاحتفاظ بنسخ من المستندات التي تم تقديمها إلى الهيئة بشأن حوادث تسرب البيانات الشخصية لديها، وتوثيق الإجراءات التصحيحية المتخذة حيالها، وأي مستندات أو وثائق داعمة ذات علاقة. وعلى جهة التحكم العمل على تصحيح الإجراءات اللازمة لاحتواء حوادث تسرب البيانات الشخصية وفقاً لمخرجات الدروس المستفادة من هذه الحوادث.

SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority