

## الالتزام بالإخطار والإبلاغ في حالة خرق البيانات

تخاطب هذه الإرشادات كل من المتحكم ومعالج البيانات.

المواد ذات الصلة: المواد 7 و 38 من قانون حماية البيانات الشخصية؛ والمواد \_\_\_\_ من اللائحة التنفيذية

توضح الارشادات:

1. التزامات المتحكم بالمعالج بالإبلاغ عن خرق البيانات أو انتهاكها أو كليهما معاً
2. المعلومات الواجب توافرها في حالة وقوع خرق للبيانات أو انتهاكها أو كليهما معاً

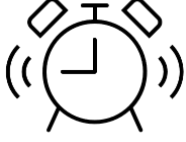
1. التزامات المتحكم والمعالج في حالة وقوع خرق للبيانات أو انتهاكها أو كليهما معاً
  - يتعين على المتحكم والمعالج إخطار مركز حماية البيانات الشخصية بأي خرق للبيانات خلال 72 ساعة من وقت العلم بحدوثه.
  - يكون كلا من المتحكم او المعالج او كليهما علي علم بالخرق عندما يتوفر لديهم قدر معقول من المعلومات يؤكد حدوث الخرق .
  - إذا كان الخرق يتعلق بالأمن الوطني، يجب أن يتم الإخطار فوراً.

يرجى الإبلاغ في حالة الخرق المتعلق بالأمن القومي على [PDPC.org](mailto:PDPC.org).

### يقوم جهاز حماية البيانات الشخصية بإبلاغ سلطات الأمن الوطني على الفور والتحقيق .

- يُعرّف القانون خرق البيانات الشخصية وانتهاكها بأنه: أي وصول غير مصرح به أو غير قانوني إلى البيانات الشخصية، أو أي عملية أخرى غير مشروعة لإعادة إنتاج أو إرسال أو توزيع أو تبادل أو نقل أو تداول تهدف إلى الكشف عن هذه البيانات الشخصية أو إفشائها أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها.
- يجب على المتحكم ومعالج البيانات إعلام الشخص المعني بالخرق خلال 3 أيام عمل من إخطار مركز حماية البيانات الشخصية.
- يجب أن يقوم المتحكمين والمعالجين بتوثيق اتفاقاتهم التعاقدية لضمان إبلاغ مركز حماية البيانات الشخصية PDPC بمعلومات محدثة في الوقت المناسب.

- عقوبات عدم الإخطار بحدوث خرق

تتراوح قيمة الغرامة في حالة عدم الاخطار/الإبلاغ فيما بين 300,000 جنيه مصري و3,000,000 جنيه مصري.	
--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

2. البيانات المطلوبة في الإخطار عن خرق البيانات أو انتهاكها أو كليهما معاً

يجب على المتحكم ومعالجي البيانات تقديم ما يلي:

- وصف للخرق/الانتهاك
- تفاصيل الاتصال بمسؤول حماية البيانات (DPO)
- التأثير المحتمل للخرق/الانتهاك
- وصف للإجراءات التصحيحية/التخفيفية (التي تم اتخاذها والتي ستُخذ)
- توثيق للخرق/الانتهاك

قد يطلب مركز حماية السانات الشخصية مستندات أو معلومات أو بيانات إضافية.

إذا لم تتوافر جميع المعلومات عند حدوث الاختراق، مثل: التأثير المحتمل، أو الوثائق اللازمة وغيرها، فلا يزال يتعين عليك إخطار مركز حماية السانات الشخصية على الفور وتقديم باقي المعلومات لاحقاً. ستعاون معك جهاز حماية السانات معك لتوفير المعلومات اللازمة في غضون فترة زمنية معقولة.

إرشادات عن المعلومات اللازم توافرها عند الإخطار / الإبلاغ	
وصف الخرق	هل هو هجوم لطلب فدية، أو هجوم احتيالي، أو غير ذلك؟
أسباب الخرق	هل فشل أي من الموظفين في مراعاة قواعد الشركة؟ هل هناك نقص في التدريب؟ وما إلى ذلك
السجلات المتأثرة	كم عدد السجلات التي تأثرت؟ هل يشمل ذلك أي حساسة؟
تحديد ما إذا كان الهجوم عالي أو منخفض المخاطر	هل من الممكن أن يترتب على ذلك سرقة الهوية؟ أو إلحاق الضرر بسلامة الأفراد؟ هل يمكن تصحيحه بسهولة؟ ما هو احتمال وقوع هجمات مماثلة أخرى؟
تقديم قائمة بالإجراءات التي تم اتخاذها أو ستُخذ لتصحيح الخرق/الانتهاك	ما هي الإجراءات الفورية التي اتخذتها لاحتواء الخرق ومنع المزيد من الأضرار؟ هل هناك حاجة لإجراء تدريب لتقليل حدوث نفس الخرق في المستقبل؟ هل تحتاج الشركة إلى الاستثمار في برامج مختلفة؟ كيف تضمن الامتثال في المستقبل؟ الخ.

إرشادات عن كيفية الإخطار	
الوصف	ما هو نوع الهجوم الإلكتروني؟
أسباب الاختراق	هل هي راجعة لعدم أداء أحد الموظفين لمهامه؟ أم عدم التدريب؟ أم غيرها من الأسباب؟
تذكر دائماً توثيق الخرق والإجراءات التصحيحية بوضوح.	

3. المعلومات المطلوبة لإخطار الشخص المعني بالبيانات بخرق البيانات أو انتهاكها أو كليهما معاً :

يتعين على المتحكمين والمعالجين توفير المعلومات التالية في رسالة واحدة:

1. وصف الواقعة بلغة بسيطة وواضحة.
2. بيانات التواصل مع مسؤول حماية البيانات.
3. الآثار التي قد تترتب على الواقعة .
4. التدابير المتخذة لمعالجة الخرق/ الانتهاك وتوجيه نصائح محددة للشخص المعني بالبيانات لحماية أنفسهم .