التدخل في حالات اختراق البيانات لائحة التخطيط

IKVKK_Y2الإصدار 1.00

.1الغرض والنطاق

.1.1شركة كارديلين لتجارة صناعة الدهانات والمواد الكيميائية المحدودة (يشار إليها فيما يلي باسم "الشركة")
اعتمدت شركتنا خطة الاستجابة لخرق البيانات الشخصية هذه (المشار إليها فيما يلي بـ "خطة الاستجابة") كجزء من إجراءات التخطيط الاستراتيجي لضمان استعدادها لاتخاذ إجراءات فورية ضد خروقات أمن البيانات، وذلك وفقًا لأحكام الإعلان المتعلق بالقرار رقم 2019/10الصادر عن مجلس حماية البيانات الشخصية بتاريخ 24/01/2019بشأن إجراءات ومبادئ الإبلاغ عن خروقات البيانات الشخصية، والذي ينص على أنه "في حالة حدوث خرق للبيانات، يتعين على مراقب البيانات إعداد خطة استجابة تتضمن بنودًا مثل الجهة التي يجب الإبلاغ إليها داخل المؤسسة، والجهة المسؤولة داخل المؤسسة عن الإخطارات الواجب تقديمها في نطاق القانون، وتقييم العواقب المحتملة لخرق البيانات، وأن هذه الخطة ستُراجع على فترات محددة". ويركز تنفيذ خطة الاستجابة في حالة حدوث أي خرق على اتخاذ إجراءات سريعة لحماية الأفراد وبياناتهم الشخصية. وتهدف شركتنا بشكل أساسي إلى تنفيذ الإجراءات التالية في حالة حدوث خرق للبيانات:

(أ) إخطار مجلس حماية البيانات الشخصية (المجلس) بخرق البيانات الشخصية دون تأخير لا مبرر له وفي غضون 72ساعة كحد أقصى بعد العلم بخرق أمن البيانات (للشركة الحق في تحديد ما إذا كانت ستخطر أم لا إذا كان من غير المحتمل أن يشكل خرق البيانات الشخصية خطرًا على الحقوق والحريات الطبيعية).

(ب) إخطار أصحاب البيانات المتضررين دون تأخير غير ضروري، ما لم يكن احتمال حدوث خرق للبيانات الشخصية يؤدي إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين منخفضًا.

.1.2هذه اللائحة:

(أ) سيتم تعميم هذا على جميع الجهات المعنية بمعالجة البيانات. ويلتزم من يعملون كمعالجين للبيانات بإخطارنا فور علمهم بأي خرق لأمن البيانات الشخصية التي يعالجونها نيابة عن شركتنا.

(ب) سيتم إبلاغ موظفينا بأحكام خطة التدخل عند بدء عملهم، وسيتم مناقشتها في اجتماعات الموظفين الدورية وجلسات التدريب لضمان إطلاع الموظفين على الخطة.

.1.3الخطوات التي يجب اتباعها في المخطط الانسيابي، والذي يشكل جزءًا من هذه اللائحة.
تم تلخيصها.

.1.4التعاريف: ترد أدناه التعاريف المطبقة على أحكام هذه اللائحة.

وهي مدرجة على النحو التالي:

.1.4.1الوعي بالخرق: يُعتبر مراقب البيانات "على علم بالخرق" عندما يكون لديه درجة معقولة من اليقين بحدوث خرق أمني يعرض أمن البيانات الشخصية للخطر.

.1.4.2الضرر: البيانات الشخصية التي تم تغييرها أو إتلافها أو لم تعد كاملة.

.1.4.3التدمير: البيانات التي لم تعد متاحة أو التي فقدها مراقب البيانات بأي شكل من الأشكال.
غير متوفر بشكل يمكنه/يمكنها استخدامه.

.1.4.4الفقدان: قد تظل البيانات متاحة، لكن المتحكم فقد السيطرة على البيانات.
لقد فقدوا السيطرة على البيانات أو الوصول إليها، أو لم يعودوا يمتلكونها.

.1.4.5خرق البيانات الشخصية هو خرق أمني ينتج عنه تدمير أو فقدان أو تغيير أو كشف غير مصرح به أو وصول غير مصرح به إلى البيانات الشخصية المنقولة أو المخزنة أو المعالجة؛

.1.4.6"فقدان البيانات المؤقت": جعل البيانات الشخصية غير قابلة للاستخدام لفترة من الزمن.
الحدث الذي تسبب في ذلك.

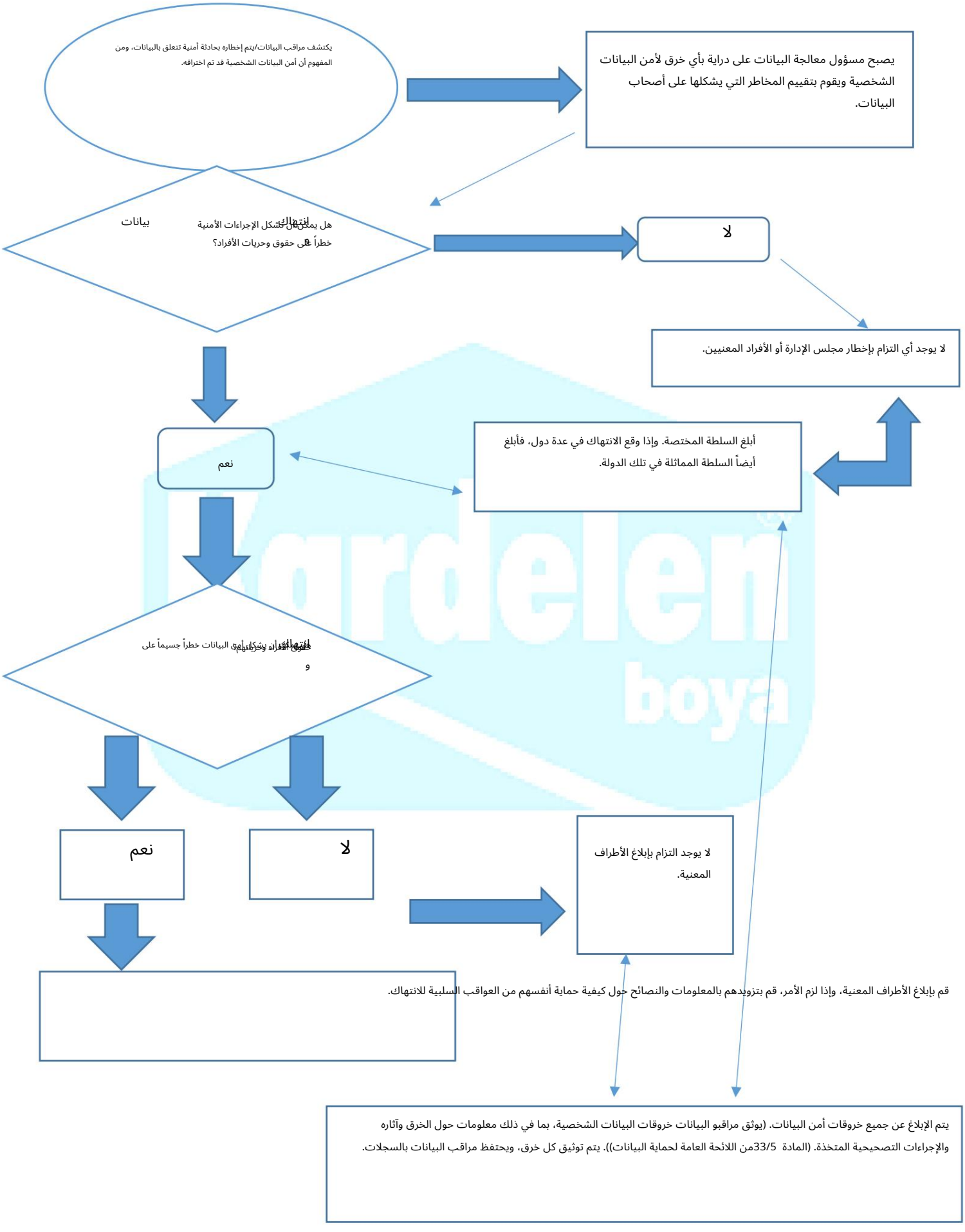
.1.4.7"المعالجة غير المصرح بها أو غير القانونية" تعني الكشف (أو الوصول) إلى البيانات الشخصية للمستلمين غير المصرح لهم بتلقي (أو الوصول) إلى البيانات، أو أي شكل آخر من أشكال المعالجة التي تنتهك أحكام القانون رقم .6698

.1.5يمكن أن يحدث خرق لأمن البيانات لأسباب متنوعة، بما في ذلك ما يلي:

- الخطأ البشري
- فقدان أو سرقة المستندات أو الأجهزة التي تحتوي على بيانات شخصية
- الدخول غير المصرح به، والسرقة، والسطو
- تطبيق ضوابط وصول غير كافية تسمح بالاستخدام/الوصول غير المصرح به
- تعطل المعدات وعدم كفاية النسخ الاحتياطية للنظام
- حالات الكوارث مثل الفيضانات أو الحرائق.
- التصيد الاحتيالي (الحصول بشكل غير قانوني على كلمة مرور شخص ما أو تفاصيل بطاقة الائتمان الخاصة به عن طريق إرسال الرسائل)، أو الاحتيال الإلكتروني، أو سرقة المعلومات، حيث يتم الحصول على المعلومات الشخصية من خلال الخداع أو الاحتيال.
- الهجمات الإلكترونية الخبيثة مثل القرصنة، والبرامج الضارة، وهجمات حجب الخدمة ،(DoS-DDoS)أو هجمات برامج الفدية.

.1.6قد تُخلّف انتهاكات البيانات الشخصية عواقب وخيمة على الأفراد، مُسببةً لهم أضرارًا جسدية أو مادية أو معنوية. وقد تُؤدي هذه الحالات إلى إحراج أو ضيق أو إذلال لصاحب البيانات. وتشمل العواقب السلبية الأخرى: فقدان السيطرة على البيانات الشخصية، وتقييد الحقوق الفردية، والتمييز، وسرقة الهوية أو الاحتيال، والخسائر المالية، والإضرار بالسمعة، وفقدان سرية البيانات الشخصية المحمية بموجب السرية المهنية، فضلًا عن أضرار اقتصادية أو اجتماعية جسيمة للأفراد المتضررين.

أ. مخطط انسيابي بشأن الالتزام بالإبلاغ عن المخالفات



1.7.يمكن أن تؤدي خروقات البيانات الشخصية إلى الحالات التالية، على سبيل المثال:
قد يضر هذا بشركتنا أيضاً:

•الإضرار بعلاقة الثقة التي بنيناها مع موظفينا وعملائنا،

•فقدان أو حذف أو تلف البيانات الشخصية اللازمة لإدارة شركتنا
رؤية،

•الإضرار بسمعة شركتنا،

•مواجهة عقوبات إدارية بموجب تشريعات حماية البيانات، أو بدء دعاوى قضائية وتحقيقات ضدنا للمطالبة بتعويضات مادية/معنوية.

2.خطة التدخل

في حالة حدوث خرق محتمل لأمن البيانات الشخصية، ستتصرف الشركة وفقًا لخطة الاستجابة الموضحة أدناه:

2.1.اكتشاف خرق أمن البيانات وإبلاغ المسؤولين المعنيين بالوضع.
2.1.1.يجب إبلاغ مسؤول الاتصال بحماية البيانات أو المدير في أسرع وقت ممكن.
سيتم ذلك.
2.1.2.يجب على مسؤول الاتصال بحماية البيانات أو المدير إخطار المدير العام على الفور.
سيوفر معلومات.
2.1.3.يقوم مسؤول/مدير الاتصال بحماية البيانات بتشكيل فريق صغير، يُشار إليه باسم فريق الاستجابة لحوادث الأمن السيبراني ،(CIRT)
لتقييم الأضرار والخسائر المحتملة، والوصول غير المصرح به، وفقدان البيانات المؤقت، واتخاذ التدابير المناسبة لاحتواء الاختراق/معالجة
الوضع واستعادة الوضع السابق للاختراق. يلتزم جميع الموظفين وجميع معالجي البيانات و/أو مراقبي البيانات المشتركين بتقديم كل المساعدة
اللازمة لمسؤول/مدير الاتصال بحماية البيانات والأفراد في الفريق الذي تم تشكيله.

2.1.4.يقوم مسؤول الاتصال/المدير المعني بحماية البيانات بإعداد تسلسل زمني مكتوب للأحداث، يسجل فيه جميع جوانب الخرق، بما في
ذلك ما يلي:

(أ) تاريخ ووقت الإبلاغ عن المخالفة (باستخدام تنسيق الوقت DD/MM/YYYYو42 ساعة).

(ب) إذا كان الإخطار يتعلق بخرق محتمل، تفاصيل التحقيق الأولي (إذا لزم الأمر) الذي سيتم إجراؤه لتحديد ما إذا كان الخرق قد
حدث بالفعل.

(ج) تفاصيل تتعلق بمن أبلغ عن الأمر.
(د) ما هو معروف / ما هو مشتبه به في هذه المرحلة الأولية.
(هـ) تفاصيل تتعلق بالنظام/مجموعة البيانات التي يرتبط بها اختراق البيانات.
(و) تقييم المخاطر التي تهدد حقوق وحريات الأشخاص الطبيعيين.

1.مسؤول الاتصال بحماية البيانات هو الشخص الذي تعينه شركتنا كمسؤول اتصال مع مجلس الإدارة، وقد يكون مديرًا كبيرًا معينًا ضمن الهيكل الإداري للشركة، أو أخصائي حماية بيانات توظفه الشركة
لهذا الغرض، أو محاميًا تعاقدنا معه لهذا الغرض.

(ز) الإجراءات التي يجب اتخاذها على وجه السرعة (التحقيق، احتواء الضرر، معالجة الوضع، استعادة البيانات، إلخ).

(ح) تفاصيل الفريق الذي تم تشكيله للمساعدة.
(أ) تفاصيل المهام الموكلة لكل عضو من أعضاء الفريق.
(ي) بنفس الطريقة المذكورة في (ز)، في غضون 72ساعة من العلم بالانتهاك، إلى المجلس سيتم إرسال الإشعار.
(ك) (إذا لزم الأمر) إخطار الأشخاص المتضررين دون تأخير لا مبرر له.

2.1.5.بغض النظر عما إذا تم اتخاذ قرار بإخطار المجلس، يجب توثيق المعلومات المتعلقة بكل خرق محتمل أو تم الإبلاغ عنه أو يُشتبه في حدوثه للبيانات الشخصية، بما في ذلك آثاره والإجراءات التصحيحية المتخذة.

2.2.الحد من الاختراق الأمني، وتخفيف آثاره، و
تدابير للقضاء على

2.2.1.ستتخذ الشركة خطوات فورية لاحتواء الاختراق وتنفيذ التدابير اللازمة لمنع الوصول غير المصرح به إلى البيانات الشخصية المحفوظة والحد من أي ضرر ناتج.

2.2.2.في حالة حدوث خرق لأمن البيانات يشمل أنظمة تكنولوجيا المعلومات و/أو البيانات الإلكترونية، سيتم الاتصال بموظفي دعم تكنولوجيا المعلومات داخل الشركة على الفور لطلب مشورتهم ودعمهم الفني فيما يتعلق بالتدابير المناسبة التي يجب اتخاذها، مثل الحد من الضرر، وعزل مناطق تخزين البيانات المتأثرة، والحفاظ على سجلات البيانات والسجلات.

2.2.3.بناءً على طبيعة الاختراق/التهديد للبيانات الشخصية، قد تشمل الإجراءات التي يتعين اتخاذها الخطوات التالية:

(أ) عزل بعض أو كل أجهزة الكمبيوتر الشخصية والشبكات وما إلى ذلك.

(ب) يجب تحذير الموظفين من عدم الوصول إلى أجهزة الكمبيوتر والشبكات والأجهزة وما إلى ذلك.

(ج) تعليق حسابات المستخدمين،

(د) التحقق من السجلات المحفوظة على خوادم النسخ الاحتياطي،

(هـ) تحديد أنواع البيانات الشخصية التي ربما تم الكشف عنها وكيف وقع حادث الوصول غير المصرح به.

2.2.4.إذا لزم الأمر، يمكن أيضًا النظر في عزل مناطق تسجيل البيانات التي يتم الحفاظ عليها يدويًا أو بطرق أخرى.

2.2.5.عند الضرورة، يمكن الاستعانة بفريق التحقيق في جرائم تكنولوجيا المعلومات ويمكن طلب المشورة القانونية.

2.3.تحليل المخاطر

2.3.1.في حالة حدوث خرق للبيانات الشخصية، تلتزم الشركة بإجراء تحليل شامل للمخاطر لتحديد ما إذا كان خرق البيانات الشخصية يشكل خطرًا على حقوق وحريات الأفراد.

2.3.2.فئات المخاطر التي ستشكل أساس التقييم هي كما يلي:

•لا يوجد خطر: إن تطبيق الضمانات التقنية والإدارية المناسبة وحماية البيانات الشخصية من خلال تدابير مثل التشفير الذي يجعل البيانات غير قابلة للقراءة لأولئك الذين ليس لديهم تصريح بالوصول إليها، إلى جانب الاحتياطات الإضافية، يضمن عدم إمكانية حدوث خطر كبير على حقوق وحريات أصحاب البيانات.

•مخاطر منخفضة: يمكن للأفراد المعنيين التغلب على المضايقات البسيطة.
قد يواجهون (قضاء وقت طويل، إزعاج، إلخ).
•خطر متوسط: قد يواجه الأفراد صعوبات يمكنهم التغلب عليها.
(جهد إضافي، تكاليف إضافية، إجهاد، انزعاج جسدي طفيف، إلخ.)
•خطر مرتفع: مرتفع: قد يواجه الأفراد عواقب وخيمة سيتعين عليهم التغلب عليها (أضرار مالية، فقدان الوظيفة، تحقيق قانوني، تدهور الصحة، إلخ).
•خطر مرتفع للغاية: قد يواجه الأفراد صعوبات لا يمكن التغلب عليها وعواقب لا رجعة فيها (توقف العمل، والضيق النفسي والجسدي طويل الأمد، والوفاة، وما إلى ذلك).

إذا تم تقييم عدم وجود خطر على حقوق وحريات الأشخاص الطبيعيين، فسيتم تسجيل الأسباب التي أدت إلى هذا التقييم.

2.3.3.عند إجراء تحليل المخاطر، ستأخذ الشركة في الاعتبار مستوى حساسية البيانات وفئات الأفراد المعنيين (مثل الأطفال والأشخاص الضعفاء) لتحديد ما إذا كانوا سيكونون أكثر عرضة للخطر بسبب الاختراق.

2.3.4.إن حقيقة أن البيانات الشخصية مشفرة بشكل آمن باستخدام أحدث طرق التشفير وأن المفاتيح لم تتعرض للاختراق في حالة حدوث خرق أمني قد تكون بمثابة أساس للاستنتاج بأن خرق البيانات لا يشكل خطراً على حقوق وحريات الأفراد وأنه ليس من الضروري إبلاغ المجلس وأصحاب البيانات.

2.3.5.في تقييم تحليل المخاطر، ستأخذ الشركة في الاعتبار توصيات مجلس الإدارة، والمركز الوطني للاستجابة لحوادث الأمن السيبراني (USOM)، ووكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA).

2.3.6.إذا تقرر أن إبلاغ مجلس الإدارة وأصحاب البيانات ليس ضرورياً، فسيتم توثيق أسباب هذا القرار، وسيتم الاحتفاظ بهذه الوثائق في الملف لتقديمها أثناء أي عمليات تدقيق قد يجريها مجلس الإدارة.

2 www.enisa.europa.eu/publications/dbn-severity

2.4.إخطار المؤسسات والأفراد المعنيين بالمخالفة

2.4.1.الإبلاغ عن حوادث اختراق أمن البيانات إلى مجلس حماية البيانات الشخصية: جميع الحوادث التي قد تكون فيها البيانات الشخصية والبيانات الشخصية الحساسة معرضة للخطر (لا يتم تضمين الحالات التي لا تشكل خطرًا على حقوق وحريات أصحاب البيانات في هذا النطاق).

سيتم إبلاغ المجلس بالحادثة دون تأخير غير مبرر وفي غضون 72ساعة كحد أقصى من الإبلاغ عن المخالفة.

2.4.2.استكمال نموذج الإبلاغ عن خرق البيانات الشخصية :KVKKبعد الوصول إلى موقع هيئة حماية البيانات الشخصية على ،www.kvkk.gov.tr انقر فوق رمز الإبلاغ عن خرق البيانات الشخصية الموجود في القوائم على الجانب الأيمن من الصفحة الرئيسية للدخول إلى منطقة الإبلاغ عن خرق البيانات الشخصية.

٢.٤.٣.تحتوي صفحة تسجيل الدخول على "إعلان بشأن قرار مجلس حماية البيانات الشخصية المؤرخ ٢٤/٠١/٢٠١٩والمرقم ٢٠١٩/١٠بشأن إجراءات ومبادئ الإبلاغ عن خروقات البيانات الشخصية". يمكنك الوصول إلى صفحة الإشعارات بالنقر على نموذج الإبلاغ عن خروقات البيانات الشخصية (عبر الإنترنت) الموجود أسفل هذه الصفحة. إذا كنت ترغب في ملء النموذج يدويًا، فانقر على نموذج الإبلاغ عن خروقات البيانات الشخصية (ملف PDF).

2.4.2.يجب أن يتضمن الإخطار المقدم إلى المجلس النقاط التالية على الأقل:

•معلومات حول مصدر المخالفة وكيفية حدوثها.
•الفئات الفردية المتضررة من الانتهاك (مثل الأطفال، والفئات الضعيفة الأخرى، والأشخاص ذوي الإعاقة،
•عدد الأشخاص والسجلات المتأثرة بخرق البيانات (على الأقل تقديري).

•فئات البيانات الشخصية المتأثرة بالاختراق (على سبيل المثال، معلومات الهوية، والسجلات التعليمية، وبيانات الضمان الاجتماعي، والمعلومات المالية، وأرقام الحسابات المصرفية، وأرقام جوازات السفر، والبيانات الصحية، بالإضافة إلى فئات خاصة من البيانات مثل العرق والإثنية)
•اسم ومعلومات الاتصال بمسؤول/مدير الاتصال بحماية البيانات (معلومات الاتصال بالمسؤول الذي يمكن الحصول منه على معلومات مفصلة)
•وصف للأثر المحتمل للاختراق على الأفراد المتضررين (على سبيل المثال، فقدان السيطرة على البيانات الشخصية، وسرقة الهوية، والتمييز، وتقييد الحقوق، والاحتيال، والخسارة المالية، والإضرار بالسمعة، وخطر الكشف عن المعلومات المهنية السرية، وما إلى ذلك).

•وصف للإجراءات الإدارية والفنية التي اتخذتها الشركة قبل الاختراق، بالإضافة إلى الإجراءات المتخذة أو المخطط لها لمعالجة الاختراق. (على سبيل المثال، حذف البيانات المنقولة عن طريق الخطأ، وتأمين كلمات المرور، والتخطيط لتدريب أمن البيانات، وما إلى ذلك). وإذا أمكن، سيتم تضمين الإجراءات المتخذة للتخفيف من الآثار السلبية للاختراق تحت هذا العنوان أيضًا.

ملاحظة هامة: إن عدم توفر معلومات نهائية بشأن المسائل المذكورة أعلاه لا ينبغي أن يؤدي إلى تأخير إخطار المجلس في الوقت المناسب. يجب التأكيد على أنه سيتم إبلاغكم بالمعلومات الحالية، وسيتم إبلاغ المؤسسة فور توفر معلومات أكثر تفصيلاً.

2.4.3.في الحالات التي يقع فيها اختراق البيانات ضمن اختصاص السلطات القضائية أو وكالات إنفاذ القانون أو غيرها من المؤسسات العامة الموجودة في الخارج، وفيما يتعلق بهذا الاختراق...

قد يلزم إبلاغ المنظمات أو المؤسسات الموجودة في الخارج. وفي حال الإبلاغ، يجب تسجيل المستندات التي تثبت ذلك وتقديمها إلى المجلس.

يجب تقديمها مع الإشعار.

2.4.4أسباب إخطار الشركة:

(أ) تجنب الغرامات الإدارية: المادة 18من القانون رقم 6698بشأن حماية البيانات الشخصية.
قد يؤدي عدم إخطار المجلس وفقًا للمادة ذات الصلة إلى غرامة إدارية.

(ب) طلب المشورة: يجوز للشركة طلب المشورة من مجلس الإدارة بشأن التدابير التي يجب اتخاذها استجابة للاختراق، والتعاون مع مجلس الإدارة أمر مهم لتبرير قراراتها بشأن إبلاغ أصحاب البيانات المتضررين أو عدم إبلاغهم.

.2.4.5إبلاغ الأشخاص المعنيين المتضررين من الخرق

.2.4.5.1بعد إجراء تحليل المخاطر المذكور في القسم 2.3.1أعلاه، إذا كان من المحتمل أن يشكل خرق البيانات الشخصية "خطرًا كبيرًا" على حقوق وحريات الأشخاص الطبيعيين، فعلى الشركة ما يلي:

(أ) سيتم الاتصال بالأطراف المعنية عبر الهاتف والبريد الإلكتروني وما إلى ذلك، دون تأخير غير ضروري.

(ب) سيتم إخطار الأفراد المعنيين بحدوث اختراق للبيانات.

(ج) سيوفر ذلك للأفراد المعنيين بالبيانات معلومات مفصلة حول الأمور المذكورة أعلاه تحت البند .2.4.2

(د) عند الاقتضاء، ستقدم نصائح محددة لأصحاب البيانات حول كيفية حماية أنفسهم من العواقب السلبية المحتملة للاختراق (مثل إعادة تعيين كلمة المرور).

.2.4.5.2يجب أن يشرح الإخطار الموجه إلى صاحب البيانات بوضوح وبساطة طبيعة خرق البيانات الشخصية، وأن يتضمن، كحد أدنى، اسم ومعلومات الاتصال بمسؤول حماية البيانات أو أي جهة اتصال أخرى يمكن الحصول منها على مزيد من المعلومات، والعواقب المحتملة لخرق البيانات الشخصية، وعند الاقتضاء، شرحًا للإجراءات التي اتخذتها شركتنا أو أوصت بها لمعالجة خرق البيانات الشخصية، بما في ذلك التدابير اللازمة للتخفيف من الآثار السلبية المحتملة لخرق البيانات الشخصية.

.2.4.6لا يُشترط إخطار صاحب البيانات إذا تم استيفاء أي من الشروط التالية:

(أ) يجب أن تكون الشركة قد طبقت ضمانات فنية وإدارية مناسبة، بما في ذلك تدابير مثل التشفير الذي يجعل البيانات الشخصية غير قابلة للقراءة لأي شخص غير مصرح له بالوصول إليها، ويجب أن تكون هذه التدابير قد تم تطبيقها على البيانات الشخصية المتأثرة بالاختراق؛

(ب) يجب على الشركة اتخاذ تدابير إضافية لضمان عدم إمكانية حدوث مخاطر عالية على حقوق وحريات أصحاب البيانات؛

(ج) إذا كان الإخطار يتطلب جهداً مفرطاً. في هذه الحالة، يُطبّق بدلاً من ذلك إخطار عام أو إجراء مماثل، يتم فيه إبلاغ أصحاب البيانات بنفس الفعالية.

2.4.7.إخطار سلطات إنفاذ القانون

(أ) في حالة الوصول غير المصرح به إلى البيانات الشخصية، يجب الإبلاغ عن الأمر فوراً إلى وكالة إنفاذ القانون المختصة.

(ب) بناءً على طبيعة البيانات الشخصية المعرضة للخطر، وخاصة عندما تكون البيانات الشخصية الحساسة معرضة للخطر، ينبغي طلب المزيد من المساعدة من جهات إنفاذ القانون.

(ج) في حالة حدوث "تلف" في البيانات، يجب الإبلاغ عن الأمر إلى جهات إنفاذ القانون. قد يؤدي عدم القيام بذلك إلى تعريض الشركة لعقوبات وإجراءات أمنية.

2.4.8.المؤسسات والمنظمات الأخرى: إذا لزم الأمر، يمكن إبلاغ وزارة الصحة، ووزارة الأسرة والسياسات الاجتماعية، والمؤسسات المالية، والوزارات والمنظمات الأخرى ذات الصلة.

2.4.9.ستقوم الشركة بإخطار شركة التأمين التي تم إبرام عقد التأمين معها وإبلاغها بخرق أمن البيانات الشخصية.

2.5.استخدام خدمات الاستشارات القانونية والمحامين: يجوز للشركة إبلاغ أصحاب المصلحة الذين تتلقى منهم خدمات الاستشارات القانونية والمحامين، وإخطارهم بخرق أمن البيانات الشخصية من أجل طلب المشورة القانونية، والدفاع في الدعاوى القضائية المحتملة، والتسوية، أو غيرها من الحلول الودية.

2.6.الإجراءات الواجب اتخاذها بعد حدوث خرق أمني: بعد اتخاذ تدابير الاستجابة الطارئة اللازمة في المرحلة الأولية، ينبغي إجراء تقييم ومراجعة شاملة للخرق الأمني في غضون فترة زمنية معقولة. وسيتم مراعاة النقاط التالية خلال هذه العملية:

2.6.1.سيتم التأكد من توثيق خروقات البيانات الشخصية، بما في ذلك المعلومات المتعلقة بخرق البيانات الشخصية وآثاره والإجراءات التصحيحية المتخذة.

2.6.2ينبغي تحديد الاستنتاجات المستخلصة من الحادث، والجوانب التي تحتاج إلى تحسين، وتفاصيل التدابير التي يتعين اتخاذها.

2.6.3يجب على الشركة أن تطلب إحاطة مناسبة وتقرير تحقيق من مسؤول الاتصال بحماية البيانات/المدعي العام (و/أو خبراء خارجيين آخرين يمكن الاستفادة من خبرتهم لمساعدتها)، ويجب الاحتفاظ بنسخة من المراسلات المتبادلة مع مجلس الإدارة و/أو الأطراف المعنية المتأثرة بالخرق.

2.6.4ستنظر الشركة بعناية فيما إذا كانت ستبدأ إجراءات تأديبية أم لا، إذا لزم الأمر.

2.6.5عندما تعتبر الإجراءات التصحيحية ضرورية، سيتم إسناد المسؤولية إلى المسؤولين المعنيين، وسيتم تكليفهم بضمان إتمام الإجراءات اللازمة في غضون أطر زمنية محددة وفقًا لمجالات مسؤوليتهم.

2.6.6يجب إبلاغ الموظفين بأي تغييرات تطرأ على خطة الاستجابة هذه وأي إجراءات أمنية محدثة. كما يجب أن يتلقى الموظفون تدريباً تنشيطياً حسب الحاجة.

الملحق -نموذج تقرير المخالفة

تقرير عن خرق أمن البيانات

للاستخدام مع دهانات كارديلين فقط.

اختراق البيانات الشخصية: يشير هذا إلى خرق أمني ينتج عنه تدمير أو فقدان أو تغيير أو الكشف غير المصرح به أو الوصول غير المصرح به إلى البيانات الشخصية التي يتم نقلها أو تخزينها أو معالجتها، سواء كان ذلك عن طريق الخطأ أو بشكل غير قانوني.

	رقم تتبع المخالفة:
	متى حدث اختراق أمن البيانات؟
الموقع الذي وقعت فيه المخالفة	أين حدث اختراق أمن البيانات؟
يرجى تحديد التاريخ والوقت.	متى تم الإبلاغ عن المخالفة؟
	من قام بالإبلاغ عن الاختراق الأمني؟
	معلومات الاتصال بالشخص الذي أبلغ عن اختراق البيانات؟
هل تم إخطار مجلس حماية البيانات الشخصية؟ نعم ☐ لا ☐	
إذا كانت الإجابة "نعم"، فيرجى تحديد طريقة الإخطار (الهاتف، البريد الإلكتروني، إلخ) وتاريخ ووقت الإخطار.	
إذا كانت الإجابة "لا"، فهل تم الاتصال بأي مسؤول كبير آخر، أو مدير، أو ما شابه، وإذا كان الأمر كذلك، فبأي وسيلة (مثل الهاتف، أو البريد الإلكتروني، وما إلى ذلك) وما هو وقت وتاريخ الاتصال؟	
هل يوجد أي شهود على الحادث؟ إذا كانت الإجابة "نعم"، فيرجى تقديم أسمائهم ومعلومات الاتصال بهم عبر الهاتف.	

يرجى تقديم معلومات حول مصدر المخالفة.
قدّم معلومات مفصلة حول كيفية وقوع المخالفة.
يرجى تقديم معلومات عن فئات الأطراف المعنية المتأثرة أو التي يُحتمل أن تتأثر بالخرق. (المتدربون، الموظفون، المتقدمون للوظائف، العملاء، الموردون، المقاولون، إلخ.)
ما هو عدد الأفراد والسجلات المتأثرة أو التي يُحتمل أن تتأثر باختراق البيانات؟ (إذا كان عدد الأفراد و/أو السجلات تقديرياً، فيُرجى توضيح سبب عدم إمكانية تحديد الأعداد الدقيقة).
ما هي فئات البيانات الشخصية التي تأثرت بالاختراق؟ (الهوية، بيانات الاتصال، الموقع، المعلومات الشخصية، الإجراءات القانونية، معاملات العملاء، الأمن المادي، أمن المعاملات، إدارة المخاطر، الشؤون المالية، الخبرة المهنية، التسويق، التسجيلات الصوتية والمرئية، العرق والإثنية، الآراء السياسية، المعتقدات الفلسفية، الملابس، عضوية الجمعيات، المعلومات الصحية، الإدانات الجنائية والتدابير الأمنية، البيانات البيومترية، إلخ.)

صف الآثار المحتملة للاختراق على الأفراد المتضررين. (فقدان السيطرة على البيانات الشخصية، سرقة الهوية، التمييز، تقييد الحقوق، الاحتيال، الخسائر المالية، الإضرار بالسمعة، فقدان أمن البيانات الشخصية، إلخ.)

يرجى وصف الإجراءات التي اتخذتها الشركة أو اقترحتها لمعالجة خرق البيانات الشخصية، بما في ذلك التدابير اللازمة للتخفيف من الآثار السلبية المحتملة لخرق البيانات الشخصية.

ملاحظة هامة: إن عدم الإلمام بالتفاصيل المتعلقة بالتدابير المذكورة أعلاه لا يبرر الامتناع عن إخطار مجلس حماية البيانات الشخصية.

يمكن تقديم المعلومات على مراحل دون أي تأخير إضافي غير ضروري. إذا كان الأمر كذلك، فيرجى التوضيح بوضوح.

هل تعتقد أن اختراق أمن البيانات حالة مؤقتة؟ هل من الممكن استعادة البيانات الشخصية المخترقة واستعادة الوصول إليها؟

هل تأثر أي نظام من أنظمة تكنولوجيا المعلومات بالحادث؟ (مثل البريد الإلكتروني، الموقع الإلكتروني، البرامج السحابية، أنظمة إدارة المستندات الإلكترونية، إلخ.) إذا كان الأمر كذلك، فيرجى سردها أدناه.
هل تتوفر أي مواد معلوماتية إضافية، مثل رسائل الخطأ، أو لقطات الشاشة، أو ملفات السجل، أو لقطات كاميرات المراقبة؟
هل اتخذت أي إجراء لإزالة/تخفيف المخاطر التي قد يتعرض لها أصحاب البيانات الذين تعتقد أنهم قد تأثروا، أو أصحاب البيانات الآخرين الذين تعتقد أنهم قد تأثروا؟ إذا كانت إجابتك "نعم"، فيرجى التوضيح أدناه.
هل أبلغت أيًا من مسؤولي الإدارة، كأحد أعضاء مجلس إدارة الشركة أو الرئيس التنفيذي أو رئيس قسم تقنية المعلومات، بهذا الأمر؟ إذا كانت الإجابة "نعم"، فيرجى وصف الشخص الذي تحدثت إليه بإيجاز، وما هي النصائح أو التعليمات التي تلقيتها خلال المحادثة.
هل تواصلت مع أي جهات خارجية، مثل شركات التأمين، أو مزودي خدمات تكنولوجيا المعلومات، أو وكالات إنفاذ القانون، وما إلى ذلك؟ إذا كانت الإجابة "نعم"، فيرجى وصف الجهات التي تواصلت معها أدناه، مع ذكر أسمائها ومعلومات الاتصال بها. .

إذا كان هناك أي شيء آخر ترغب في توضيحه، فيرجى ذكره أدناه.

حرره:	
مهمتك:	
كوارث وحدة:	
معلومات الاتصال الخاصة بك: (يفضل رقم هاتفك)	
تاريخ:	
وقت إنجاز التقرير:	

نشكركم على جهودكم في تعبئة هذا النموذج. ستساعد تعبئة هذا النموذج كارديلين بويا على التحقيق في الأمر وتحليله بشكل أفضل.
يرجى التأكد من إرسال هذا التقرير مباشرة إلى مسؤول الاتصال بحماية البيانات/الأستاذ في الشركة:
مسؤول/مدير الاتصال بحماية البيانات: الاسم واللقب: المنصب: العنوان: رقم الهاتف:
بريد إلكتروني:

*تم إعداد هذا النموذج مع مراعاة القضايا المدنية والجنائية.

للعلم:

يتم تصنيف خروقات أمن البيانات وفقًا لمبادئ أمن المعلومات المقبولة عمومًا التالية:

أ) خصوصية البيانات: يشير هذا إلى منع وصول الأشخاص غير المصرح لهم إلى البيانات. ويُقصد بـ"خرق السرية" الكشف غير المصرح به أو العرضي عن البيانات الشخصية أو الوصول إليها.

ب) سلامة البيانات: يشير هذا إلى ضمان الحفاظ على البيانات وحمايتها بالطريقة التي ينبغي أن تكون عليها.
يشير مصطلح "انتهاك السلامة" إلى التغييرات غير المصرح بها أو العرضية التي تطرأ على البيانات الشخصية.

ج) إمكانية الوصول إلى البيانات/توافرها: يشير هذا إلى إمكانية الوصول إلى البيانات واستخدامها في جميع الأوقات. ويُقصد بـ"خرق الوصول" فقدان الوصول إلى البيانات الشخصية عن طريق الخطأ أو دون إذن، أو إتلاف البيانات الشخصية عن طريق الخطأ أو دون إذن.

بحسب الظروف، قد يحدث خرق لأمن البيانات نتيجة انتهاك سرية البيانات الشخصية أو سلامتها أو توافرها، أو مزيج من هذه العوامل. وتكون المعلومات التي تساعد في تحديد ما إذا كان قد حدث خرق للسرية أو السلامة واضحة نسبيًا. مع ذلك، قد يكون تحديد ما إذا كان قد تم انتهاك توافر البيانات أكثر صعوبة. وعندما تُفقد البيانات الشخصية أو تُتلف نهائيًا، يُعتبر ذلك دائمًا انتهاكًا لمبدأ توافر البيانات.

الإجراءات الواجب اتباعها عند الاستجابة للاختراقات الأمنية.

أشياء لا يجب عليك فعلها:

أشياء للقيام بها:

•المزيد من الوصول غير المصرح به، والكشف عن البيانات، وإلحاق الضرر بأنظمة السجلات، وما إلى ذلك.
لمنع وقوع المزيد من الحوادث، قم بعزل النظام المتضرر على الفور.
•استخدم هاتفك للتواصل. يمكن للمهاجمين مراقبة حركة البريد الإلكتروني.
•اتصل بمسؤول/مدير حماية البيانات في الشركة على الفور.

مسؤول/مدير الاتصال بحماية البيانات:

الاسم واللقب:

مسمى وظيفي:

عنوان:

رقم الهاتف:

بريد إلكتروني:

•الاحتفاظ بجميع سجلات النظام ذات الصلة، على سبيل المثال، جدار الحماية، وجهاز التوجيه، ونظام كشف التسلل.

•قم بإنشاء نسخ احتياطية من الملفات التالفة أو المعدلة واحفظ هذه النسخ الاحتياطية.
احتفظ به في مكان آمن.
•تحديد مكان النظام المتأثر داخل بنية الشبكة.
•تحديد جميع الأنظمة والوحدات المتصلة بالنظام المتأثر.
•البرامج والعمليات التي تعمل على النظام (الأنظمة) المتأثرة، وتأثير الانقطاع، والصلاحيات
حدد الحد الأقصى المسموح به لمدة انقطاع الخدمة.
•في حالة جمع الأدلة على النظام المتأثر، قم باتخاذ الترتيبات اللازمة لضمان استمرارية الخدمة، أي قم بإعداد نظام احتياطي وإنشاء نسخ احتياطية للبيانات.

أشياء لا يجب عليك فعلها:

•لا تقم بحذف أو نقل أو تعديل الملفات على الأنظمة المتأثرة. •لا تتصل بالمهاجمين المشتبه بهم. •لا تقم بتحليل الجرائم الإلكترونية إلا إذا كنت مخولاً بذلك.

يجب تعبئة هذا النموذج فقط من قبل فريق الاستجابة لخرق البيانات.

مسؤول/مدير الاتصال بحماية البيانات:	
	تاريخ ووقت تقديم هذا النموذج إلى الشركة:
	يرجى تحديد مدى تأثير اختراق أمن البيانات. خصوصية البيانات، سلامة البيانات، الوصول إلى البيانات/توافرها (انظر التوضيحات أعلاه)
ما هو العدد التقديري للأفراد والسجلات المتأثرة بالاختراق؟ ما هي فئات البيانات المتأثرة؟	عدد الأفراد والسجلات المتأثرة باختراق البيانات
نعم ☐ لا ☐ هل تأثرت البيانات الشخصية الحساسة التي تأثرت (العرق والأصل الإثني، والرأي السياسي، والمعتقدات الدينية والفلسفية، والانتماء الطائفي وغيره من المعتقدات، والانتماءات النقابية، والبيانات البيومترية والوراثية، والمعلومات الصحية، والبيانات الجنسية)؟ يرجى كتابة المعلومات ذات الصلة أدناه. على سبيل المثال، كم عدد فئات البيانات الشخصية الحساسة للأفراد التي تأثرت بالاختراق؟ تأثرت (الحياة).	نتيجةً لاختراق البيانات، ما هي فئات البيانات الشخصية الحساسة التي تأثرت (العرق والأصل الإثني، والرأي السياسي، والمعتقدات الدينية والفلسفية، والانتماء الطائفي وغيره من المعتقدات، والانتماءات النقابية، والبيانات البيومترية والوراثية، والمعلومات الصحية، والبيانات الجنسية)؟ يرجى كتابة المعلومات ذات الصلة أدناه. على سبيل المثال، كم عدد فئات البيانات الشخصية الحساسة للأفراد التي تأثرت بالاختراق؟
مرتفع جداً: قد يواجه الأفراد صعوبات لا يمكن التغلب عليها وعواقب لا رجعة فيها (توقف العمل، ضائقة نفسية وجسدية طويلة الأمد، الموت، إلخ).	احتمالية تعرض الأفراد المعنيين لآثار سلبية. يشكل التدمير العرضي أو غير القانوني أو الفقدان أو التغيير أو الكشف غير المصرح به أو الوصول غير المصرح به إلى البيانات الشخصية المنقولة أو المخزنة أو المعالجة خرقًا أمنيًا. ينبغي تحديد مدى الاختراق من خلال تقييم أثره المحتمل على الأفراد المتضررين. ويجب أن يشمل هذا التقييم طبيعة الاختراق وسببه، ونوع البيانات المعنية، والتدابير المتخذة للتخفيف من آثاره، وفئات الأفراد المتضررين. *في حال عدم تقييم المخاطر، يرجى توضيح الأسباب:
مرتفع: قد يواجه الأفراد المعنيون عواقب وخيمة سيتعين عليهم التغلب عليها (أضرار مادية، فقدان الوظيفة، تحقيق قانوني، تدهور الصحة، إلخ).	
متوسط: قد يواجه الأفراد انتكاسات يمكن التعامل معها (جهد مفرط، تكاليف إضافية، إجهاد، انزعاج جسدي طفيف، إلخ).	
منخفض: قد يواجه الأفراد انتكاسات طفيفة يمكنهم التغلب عليها (مثل قضاء الكثير من الوقت، الملل).	
لا يوجد خطر: إن تطبيق الضمانات التقنية والإدارية المناسبة، وحماية البيانات الشخصية من خلال تدابير مثل التشفير الذي يجعلها غير قابلة للقراءة لأي شخص غير مصرح له بالوصول إليها، يضمن عدم وجود خطر كبير على حقوق وحريات أصحاب البيانات.	

نعم ☐لا ☐	هل تم إبلاغ كبار المسؤولين التنفيذيين في مجلس الإدارة؟
نعم ☐لا ☐	هل تم إبلاغ مزود خدمة تكنولوجيا المعلومات/فريق الدعم الفني لتكنولوجيا المعلومات؟
نعم ☐لا ☐	هل تم إبلاغ شركة التأمين؟
نعم ☐لا ☐	هل تم تقديم بلاغ/شكوى إلى جهات إنفاذ القانون؟
نعم ☐لا ☐	هل تم إبلاغ المستشارين القانونيين؟
نعم ☐لا ☐	هل تم إبلاغ الأفراد المعنيين؟ عدد الأشخاص المعنيين؟ هل توجد أي قوائم اتصال تمكننا من الوصول إلى الأشخاص المعنيين؟ أو هل من الممكن استعادة معلومات الاتصال؟
نعم ☐لا ☐ إذا كانت الإجابة "نعم"، فيرجى تضمين تاريخ ووقت الإشعار (إن وجد). اكتب النصائح والتعليمات التي تلقيتها من المؤسسة أدناه:	هل تم إخطار مجلس حماية البيانات الشخصية؟ هيئة حماية البيانات الشخصية رقم الهاتف: 00 50 216 0312 مركز الاتصال: مركز المعلومات والاستشارات لخط المساعدة الخاص بحماية البيانات ALO 198 البريد الإلكتروني: veriguvenligi@kvkk.gov.tr صفحة الويب التي تحتوي على نموذج إشعار المخالفة: Icerik/5362/Ve https://www.kvkk.gov.tr/ إشعار اختراق ri العنوان: حي نصوح عكار، شارع .1407 رقم 06520 ،4جانكايا/أنقرة
	نقاط أخرى جديرة بالملاحظة
	توقيع مسؤول/مدير الاتصال بحماية البيانات:
	الرئيس التنفيذي أو المعين توقيع الممثل:
	تاريخ:

*هذا النموذج مخصص للاستخدام في القضايا المدنية والجنائية.

تم إعداده من خلال توفيره.