تأثير حماية البيانات
إجراءات التقييم و
حول مبادئها
أنظمة

IKVKK_Y3الإصدار 1.00

شركة كارديلين المحدودة لتجارة صناعة الدهانات والمواد الكيميائية

تقييم أثر حماية البيانات (DPIA)
اللوائح المتعلقة بالإجراءات والمبادئ

.1مقدمة ونطاق البحث

.1.1يجب تقييم هذه اللائحة المتعلقة بإجراءات ومبادئ تقييم أثر حماية البيانات (DPIA)(المشار إليها فيما يلي باسم اللائحة) جنبًا إلى جنب مع سياسة أمن المعلومات الخاصة بشركتنا، وسياسة حماية البيانات الشخصية، والسياسة الإطارية.

.1.2يحكم هذا النظام الإجراءات والمبادئ التي يجب اتباعها عندما يُطلب من شركتنا، بصفتها مراقب البيانات، إجراء تقييم لتأثير أنشطة المعالجة المخطط لها على حماية البيانات الشخصية قبل نشاط المعالجة (المادة 35من اللائحة العامة لحماية البيانات)، أو عندما يقوم مالكو أصول المعلومات بإجراء تقييمات تأثير حماية البيانات خلال عمليات المراجعة السنوية لأصول المعلومات التي يتحكمون بها، لا سيما عند استخدام تقنيات جديدة من حيث منهجية تكنولوجيا المعلومات والاتصالات أو الاستخدام التجاري العام، وعندما يكون من المحتمل أن يشكل نوع من المعالجة خطرًا كبيرًا على حقوق وحريات الأشخاص الطبيعيين، مع مراعاة طبيعة ونطاق وسياق وأغراض نشاط معالجة البيانات.

.1.3التعاريف: لأغراض هذا النظام، تعتبر أصول المعلومات أصولاً مملوكة لشركة Kardelen Boyaضرورية لاستمرار عملياتها دون انقطاع، وبالتالي فهي ملزمة بحمايتها.

.1.4مالك أصول المعلومات: مدير مجال العمل الذي يتم فيه استخدام الأصل ذي الصلة.

.2تقييم أثر حماية البيانات

.2.1الموظفون المعينون كمالكين لأصول المعلومات مسؤولون عن إدارة أصول المعلومات الخاضعة لسيطرتهم وفقًا للمسؤوليات الموضحة في سياسة الإطار.

.2.2يجب على مالكي أصول المعلومات إجراء تقييم للأثر مرة واحدة على الأقل في السنة، وخاصة عندما تكون هناك تغييرات كبيرة في أصول المعلومات، أو طرق تخزينها ومعالجتها، أو تغييرات في اللوائح القانونية أو السياسات التي تتوقع تغييرات في البيانات الشخصية المخزنة داخل أصول المعلومات، يجب عليهم إجراء تقييم للأثر قبل تنفيذ أي تغييرات.

2.3.يجب على مالكي أصول المعلومات التأكد من أن أمن الأصول التي يتحكمون بها يفي بالشروط التالية المذكورة في سياسة أمن المعلومات الخاصة بالشركة:

•يجب على جميع المستخدمين التأكد بشكل صحيح من حصولهم على إمكانية الوصول إلى المعلومات قبل القيام بذلك. يجب أن يكونوا مخولين.
•اعتبار معقول يتوافق مع قيمة و/أو حساسية أصول المعلومات.
يجب ضمان مستوى معين من الأمن.

يجب على المستخدمين الإبلاغ عن أي حادثة تؤدي، أو يُحتمل أن تؤدي، إلى خرق أمني للبيانات إلى مسؤول الاتصال بحماية البيانات ومدير تقنية المعلومات. كما يجب على المستخدمين المتضررين إبلاغ فريق دعم تقنية المعلومات، أو رؤساء أقسامهم، أو كبار المسؤولين التنفيذيين في الشركة عن الخرق دون تأخير.

•يلتزم المستخدمون بإجراء تقييم لأثر حماية البيانات (DIA)على أصولهم كجزء من المراجعة السنوية لجرد أصول المعلومات الخاصة بهم.

2.3.1.يلتزم كل مالك لأصل معلوماتي ببذل جهود معقولة لضمان أن جميع المواد التي بحوزته تفي بالمتطلبات التالية في جميع الأوقات:

•يجب أن تكون البيانات التي تم جمعها قانونية.

•الالتزام بشروط استخدام موارد تكنولوجيا المعلومات، كما هو موضح في القسم 11من سياسة أمن المعلومات الخاصة بالشركة، أمر مطلوب.

•يجب ألا تحتوي البيانات التي يتم جمعها على روابط تؤدي إلى مواد غير قانونية، ويجب ألا تحتوي على محتوى يتعارض مع شروط استخدام الشركة لأدوات المعلومات والاتصالات.

•ما لم يوافق رئيس القسم المختص، لا يجوز نشر أي ترويج أو تعليق على أي سلع أو منتجات أو خدمات نيابة عن الشركة.

•ما لم تتم الموافقة من قبل رئيس القسم المختص، أو مالك أصول المعلومات، أو شركة أي شخص آخر، أو شراكة، أو اتحاد، أو شركة استشارية، أو أي معلومات و/أو بيانات تحتوي على مواد ترويجية أو تعليقات حول أنشطتهم "الخاصة"، فلا ينبغي تضمينها.

2.3.2.المعلومات التي تخص أي فرد والتي تُدرج ضمن أصول المعلومات الخاصة بالشركة و
بيانات:

•يجب ألا يحتوي على العلامة التجارية للشركة أو شعارها أو ترويسة رسائلها، إلخ.

•يجب أن تكون المواد المحفوظة مرتبطة بشكل مباشر أو ذات صلة بتفويض مالك أصول المعلومات لاستخدام أصول تكنولوجيا المعلومات الخاصة بالشركة.

•بغض النظر عن كيفية الإشارة إليها، فإن سياسات الشركة ولوائحها ذات الصلة والطريقة التي يتم بها عرض المعلومات المحفوظة بشكل فردي لا ينبغي تفسيرها بأي شكل من الأشكال على أنها تعني أن الشركة تتحمل أي مسؤولية عن المعلومات المحفوظة بشكل فردي أو أي مواد أو آراء واردة فيها أو تؤيدها.

بالنسبة لجميع المعلومات المحفوظة بشكل فردي، يجب عرض إخلاء مسؤولية معتمد على الشاشة يشير إلى أن هذه المعلومات لم يتم إصدارها رسميًا من قبل الشركة.

2.4.يتحمل جميع الموظفين مسؤولية اتباع أفضل ممارسات أمن المعلومات لضمان حماية المعلومات التي تحتفظ بها الشركة بشكل سليم، بغض النظر عن شكلها. كما يتحمل جميع رؤساء الأقسام مسؤولية الإشراف على ممارسات أمن المعلومات داخل أقسامهم كجزء من مسؤولياتهم الإدارية. وفي إطار هذه العملية، يقوم رؤساء الأقسام بمراجعة الأصول الموجودة داخل أقسامهم، وهم ملزمون بتطبيق التدابير والضوابط اللازمة لضمان أن يعكس جرد أصول المعلومات في الشركة بدقة جميع الأصول المُدارة.

2.5.يساعد جرد أصول المعلومات الإدارات المعنية في تحديد الدعم التقني اللازم لأصول المعلومات المحددة، وذلك فيما يتعلق بأمن تكنولوجيا المعلومات والاتصالات وإدارة أصولها، وفي تطبيق ضوابط أمن المعلومات. مع أن مدير تقنية المعلومات هو المسؤول عن إدارة جرد أصول المعلومات، إلا أنه ينبغي اتخاذ الاحتياطات اللازمة، مع مراعاة أمن السجلات والأصول المحفوظة ورقياً.

2.6.ينبغي تحديد أصول المعلومات باستخدام الروابط المنطقية وأساليب التجميع. على سبيل المثال، قد تُخزَّن المعلومات التي جُمعت لدراسة الصحة والسلامة والبيئة على وسائط تخزين متنوعة، بما في ذلك مجموعة من أجهزة الكمبيوتر المحمولة، ومجموعة من محركات الأقراص، ومحركات أقراص .USBفي هذه الحالة، يجب تسجيل مدخل يصف كل وسيط وكيفية الحفاظ على أمانه.

2.7.يجب على كل قسم معنيّ الإفصاح عن أصول المعلومات التي يمتلكها والتأكد من تسجيلها في قائمة الجرد. يجب تسجيل كل نظام تخزين إضافي يتم اقتناؤه محليًا لأغراض التخزين الرقمي/السجلات كأصل من أصول "النظام المستخدم من قبل القسم". في حال وجود أي شك حول ضرورة تسجيل أصول معلومات إضافية، يُرجى التواصل مع فريق دعم تقنية المعلومات. كما يجب تعريف أنظمة التخزين السحابي وأنظمة الملفات الورقية كأصول معلومات وتسجيلها في قائمة الجرد.

2.8.عند مراجعة أصول المعلومات الخاصة بأقسامهم، ينبغي على رؤساء الأقسام مراعاة ما يلي:

•هل هناك أي أصول معلوماتية تحتاج إلى إضافتها إلى المخزون؟

•أي أصول معلوماتية غير مستخدمة وتحتاج إلى إزالتها من المخزون
هل هذا ممكن؟

•هل هناك تغيير في استخدام أصول المعلومات يتطلب تحديث السجلات في قائمة جرد أصول المعلومات؟

•هل هناك أي تغييرات في السياسات أو اللوائح القانونية التي تتوقع تغييرًا في كيفية جمع ومعالجة أصول المعلومات التي تستخدمها الإدارة؟

2.9.من المعلوم أن رؤساء الأقسام قد لا يمتلكون معرفة شاملة بجميع المعلومات التي يتعامل معها موظفو أقسامهم، أو بجميع العناصر التي تُخزَّن فيها تلك المعلومات. لذا، يُوصى الأقسام، عند إعداد سجل أصول المعلومات الخاص بها، بإيلاء اهتمام واسع للمخاطر الأساسية المرتبطة بالمعلومات التي تحتفظ بها القسم، ومكان تخزينها. وقد تجد الأقسام أنه من المفيد التركيز على نقل البيانات، لا سيما البيانات الحساسة أو المنقولة خارج الكلية. يُرجى التواصل مع فريق أمن تقنية المعلومات للحصول على مزيد من الإرشادات.

3.هيكل جرد أصول المعلومات

التفسيرات	اسم النطاق
من المسؤول عن المعلومات المخزنة في أصل البيانات هذا، ومن هو جهة الاتصال/مسؤول الاتصال للاستفسارات المتعلقة بأصل البيانات هذا؟	معلومات مالك الأصل
تم تحديد دور مدير أصول المعلومات في وثيقة سياسة إطار عمل نظام إدارة أمن المعلومات، ويمكن وصفه بأنه الشخص الأكثر تفويضًا الذي يستخدم أصول المعلومات بشكل يومي.	مدير أصول المعلومات
الاسم المحدد المخصص لأصل المعلومات	اسم أصل المعلومات
قدّم وصفًا موجزًا لأصل المعلومات. وإذا أمكن، أضف ملاحظة معلوماتية قصيرة حول المعلومات التي سيتم تخزينها داخل هذا الأصل.	تعريف أصول المعلومات
لا تظهر الحالة الحالية للأصل إلا في قائمة جرد أصول المعلومات -مؤقت، معتمد، أو غير نشط، إلخ.	
•هل تحتوي أصول المعلومات على فئات خاصة من البيانات؟ ما هي المخاطر المرتبطة بهذه البيانات؟ وما هي الإجراءات المتخذة للقضاء على هذه المخاطر أو التخفيف من حدتها؟ البيانات التي سيتم اعتبارها بيانات من فئة خاصة هي كما يلي: oالبيانات المتعلقة بإدارة الشركة أو البحث الذي يعتبر بيانات حساسة تجارياً.	تصنيف

بيانات. يشير هذا إلى "البيانات المتعلقة بعرق الأفراد، وأصلهم العرقي، وآرائهم السياسية، ومعتقداتهم الفلسفية، ودينهم، وطائفتهم أو معتقداتهم الأخرى، ومظهرهم وملابسهم، وعضويتهم في الجمعيات أو المؤسسات أو النقابات العمالية، وصحتهم، وحياتهم الجنسية، وإداناتهم الجنائية، وتدابيرهم الأمنية، فضلاً عن البيانات البيومترية والوراثية" كما هو محدد في المادة 6من القانون رقم .6698 أي البيانات المالية الفردية؛ أي البيانات المتعلقة بالدراسات البحثية التي كلفت بها الشركة. تطوير ينبغي أيضًا النظر في البيانات الشخصية غير المدرجة أعلاه، والتي قد تتسبب في ضرر أو تسيء إلى سمعة الأفراد المعنيين في حال الكشف عنها، ضمن هذه الفئة.	
إلكترونياً، يدوياً، أو كليهما.	مكان تخزين الأصل نوع البيئة
ما هو الأساس القانوني لمعالجة و/أو تخزين البيانات ذات الصلة؟ وفقًا للقانون رقم ،6698يجب مراعاة أسس معالجة البيانات المشروعة التي يمكن أن يستخدمها مراقبو البيانات من أجل معالجة البيانات الشخصية بشكل قانوني.	الأساس القانوني
الأهمية الحيوية لأصول المعلومات بالنسبة لسير عمل الشركة ومستوى العواقب السلبية التي قد تنشأ في حالة فقدان هذه الأصول أو انتهاك سريتها.	من منظور سير العمل أهميته
موقع أصول المعلومات: أين يتم تخزين أصول المعلومات فعلياً؟ على سبيل المثال، على أجهزة الكمبيوتر المحلية، أو في النظام المركزي، أو في البوابة، أو في موقع آخر غير الخادم؟	
الشخص الذي أدخل السجل ذي الصلة في قائمة جرد أصول المعلومات من هذا؟	إضافة أصول المعلومات جانب
إلى متى سيتم الاحتفاظ بأصول المعلومات في المخزون؟ ما هي الآلية المتوقعة لتحديد أن المعلومات لم تعد ضرورية لعمليات الشركة ولإتلافها بشكل آمن؟ يرجى مراجعة سياسة الشركة بشأن الاحتفاظ بالبيانات وإتلافها فيما يتعلق بالمدة الزمنية التي يجب بعدها إتلاف البيانات.	التخزين المتوقع مدة
تاريخ أقدم سجل لا ينبغي أن يكون ضمن نطاق فترة الاحتفاظ بالتاريخ الحالية.	أقدم إدخال
تاريخ آخر إدخال لأصول المعلومات التي لم تعد تُحدَّث.	آخر إدخال مسجل

يجب على المسؤولين المعينين كمالكين لأصول المعلومات مراعاة ما يلي أيضًا:

•الوحدة المسؤولة: ما هي الوحدة المسؤولة عن أصل المعلومات المعني؟ (عادةً ما تكون الوحدة المسؤولة عن "مالك الأصل").

•ما هي الوحدات و/أو الأفراد الذين سيتمكنون من الوصول إلى أصول المعلومات؟ يرجى تحديد مجموعات الأفراد المتوقع أن يكون لديهم حق الوصول إلى أصول المعلومات ذات الصلة. على سبيل المثال، الموظفون المعينون في فريق معين أو جميع موظفي الشركة. بالإضافة إلى ذلك، يجب تحديد الأطراف الثالثة التي ليست من موظفي الشركة ولكن من المتوقع أن يكون لديها حق الوصول إلى أصول المعلومات ذات الصلة بشكل واضح.

•كيف سيتم ضمان أمن أصول المعلومات؟ لخص الإجراءات المتخذة لضمان أمن أصول المعلومات. على سبيل المثال، الحماية بكلمة مرور. هل تُحفظ السجلات التي تحتوي على بيانات شخصية حساسة في شكل ورقي في نظام ملفات مقفل؟ كيف تتم صيانة الأقفال؟ تحذير: لا تفصح تحت أي ظرف من الظروف عن مكان تخزين كلمات المرور أو الأقفال! •ترتيبات النسخ الاحتياطي، والمرونة، والتعافي من الكوارث: ما هي الإجراءات المتخذة لاستعادة البيانات و/أو الحفاظ على وظائف البيانات وإمكانية الوصول إليها في حالة فقدان البيانات أو اختراق أمن البيانات/الأنظمة، أو في حالة وقوع كوارث، مثل الزلازل، وما إلى ذلك؟