جلسة توعوية عن قانون حماية البيانات الشخصية

المحتوى

- المقدمة
- الجهة الرقابية المختصة
- اهداف قانون حماية البيانات الشخصية
- الغرامات والعقوبات
- النطاق
- البيانات الشخصية
- البيانات الحساسة
- بيانات الصحة والائتمان
- اصحاب البيانات
- معالجة البيانات
- المتحكم
- التزامات المتحكمين
- المعالج
- الأساس القانوني لمعالجة البيانات
- مبادئ معالجة البيانات
- حقوق صاحب البيانات
- الإعفائات
- نقل البيانات خارج المملكة العربية السعودية
- تقييم تأثير حماية البيانات
- سجل عمليات معالجة البيانات
- دورة حياة البيانات
- مسؤول حماية البيانات والمسؤوليات
- مسؤوليات DPO
- إشعار اختراق البيانات

المقدمة

صدر نظام حماية البيانات الشخصية في المملكة العربية السعودية بموجب المرسوم الملكي رقم (م/١٩) بتاريخ ٩ / ٢ / ١٤٤٣هـ (١٦ سبتمبر ٢٠٢١م). دخل النظام حيز التنفيذ في ١٤ سبتمبر ٢٠٢٣م، مع مهلة سنة لتحقيق الامتثال حتى ١٤ سبتمبر ٢٠٢٤م.

يهدف إلى

حماية الخصوصية الفردية

تنظيم جمع البيانات الشخصية ومعالجتها وتخزينها والإفصاح عنها والاحتفاظ بها

يتضمن متطلبات مفصلة على

مبادئ المعالجة ، حقوق صاحب البيانات ، الالتزامات التنظيمية والنقل عبر الحدود

الجهة الرقابية المختصة

الهيئة السعودية للبيانات والذكاء الاصطناعي(SDAIA)

- إصدار الإرشادات واللوائح التنفيذية والقواعد التكميلية ، مثل لوائح نقل البيانات الشخصية.
- الموافقة على نقل البيانات عبر الحدود عند عدم توفر الحماية الكافية.
- مراقبة الامتثال من خلال عمليات التدقيق والتحقيقات.
- التعامل مع شكاوى أصحاب البيانات وضمان حقوقهم بموجب قانون حماية البيانات وحماية البيانات العامة.
- إدارة السجل الوطني للمراقبين للمؤسسات التي تعالج البيانات الشخصية.

اهداف قانون حماية البيانات الشخصية

يهدف قانون حماية البيانات الشخصية إلى تلخيص ما يلي :

- تبسيط قوانين الخصوصية المختلفة الخاصة بالقطاع بموجب قانون واحد
- خصوصية البيانات الشخصية للمقيمين في المملكة العربية السعودية
- منع إساءة استخدام البيانات الشخصية
- تنظيم ممارسات مشاركة البيانات
- دعم الابتكار لتنمية الاقتصاد الرقمي
- تطوير البنية التحتية الرقمية

الغرامات والعقوبات

- إذا قام فرد بالإفصاح عن بيانات حساسة أو نشرها بما يخالف قانون حماية البيانات أو الحصول على منفعة شخصية، فقد يواجه: السجن لمدة تصل إلى عامين أو غرامة تصل إلى ٣ ملايين ريال أو كليهما. في حالات التكرار ، يمكن مضاعفة الغرامات من قبل المحكمة.

- بالنسبة للمخالفات العامة، قد يتعرض أي فرد (طبيعي أو قانوني) يخالف قانون حماية التعويض او قانون حماية الممتلكات أو لوائحه: إنذار أو غرامة تصل إلى ٥ ملايين ريال. في حالات التكرار ، يمكن مضاعفة الغرامات من قبل المحكمة.

- يمكن للأفراد الذين يعانون من أضرار بسبب هذه الانتهاكات طلب تعويض متناسب في محكمة مختصة عن الأضرار المادية أو المعنوية.
[المادة ٤٠ من قانون قانون حماية الحقوق المدنية والعامة]

النطاق

يشمل القانون جميع الجهات التي تعالج البيانات الشخصية للمجموعات التالية:

- مواطني المملكة العربية السعودية.
- المقيمين، بما في ذلك العمال المؤقتين والدائمين.
- الزوار المؤقتين، مثل السياح.
- أي شخص يقيم في المملكة لأي سبب ولفترة زمنية غير محددة.

- يرجى ملاحظة أنه حتى إذا غادر الفرد أراضي المملكة، فإن بياناته الشخصية ستظل ضمن نطاق قانون حماية البيانات الشخصية إذا كانت هذه البيانات الشخصية لا تزال مخزنة في المملكة.
- كما يشمل القانون بيانات الأشخاص المتوفين إذا كانت تحددهم بشكل مباشر أو تحدد أفراد عائلتهم.

البيانات الشخصية ؟

تشير البيانات الشخصية إلى معلومات التعريف عن الأفراد.

تصبح نقطة البيانات بيانات شخصية عندما تحدد هوية الشخص مباشرة.

تصبح البيانات أيضا بيانات شخصية عندما تحدد هوية الشخص بشكل غير مباشر.

البيانات الشخصية | تحديد هوية الفرد بشكل غير مباشر

قسم الأمن المادي يخزن:

نظام 1 – قاعدة البيانات أ :

البيانات الشخصية
اسم
رقم الهاتف
معرف الموظف
معلومات السيارة (#)

نظام ٢ – قاعدة البيانات ب :

وقت الخروج	وقت الدخول	معلومات السيارة (#)
٠٥:٠٠	٠٩:٠٠	7413 أ و ى
٠٤:١٥	٠٨:٤٥	٢٠٣٠ ج ي د

تستخدم للهوية وإدارة كشوف الرواتب وأيضاً تستخدم لإصدار تحذيرات لمخالفات وقوف السيارات.

البيانات الشخصية

* كما هو محدد في المادة ١(٤) في PDPL

أي بيانات، بغض النظر عن مصدرها أو شكلها، قد تؤدي إلى تحديد هوية الفرد على وجه التحديد، أو التي قد تجعل **من الممكن بشكل مباشر أو غير مباشر تحديد هوية الفرد**، بما في ذلك الاسم ورقم التعريف الشخصي والعناوين وأرقام الاتصال وأرقام الترخيص والسجلات والأصول الشخصية وأرقام البنوك وبطاقات الائتمان والصور ومقاطع الفيديو الخاصة بالفرد وأي بيانات أخرى ذات طبيعة شخصية.

- ***ما يعرف الفرد المحدد :*** *الاسم والبريد الإلكتروني والجوال #، وجواز السفر #، الإقامة # إلخ.*
- ***من الممكن تحديد هوية الفرد المحدد :*** *المنزل # ، السيارة # ، عنوان IP ، جهاز MAC إلخ.*

البيانات الحساسة

* كما هو محدد في المادة ١(١١) في PDPL

تشمل البيانات الحساسة :

- الأصل العرقي أو المعتقد الديني أو الفكري أو السياسي.
- البيانات المتعلقة بالإدانات والجرائم الجنائية الأمنية.
- البيانات البيومترية أو الجينية لغرض تحديد هوية الشخص.
- البيانات الصحية.
- البيانات التي تشير إلى أن أحد والدي الفرد أو كلاهما غير معروفين.

البيانات الصحية والائتمانية

البيانات الصحية * كما هو محدد في المادة ١ (١٣) في PDPL

أي بيانات شخصية تتعلق بالحالة الصحية للفرد، سواء كانت ظروفه الجسدية أو العقلية أو النفسية، أو المتعلقة بالخدمات الصحية التي يتلقاها هذا الفرد.

البيانات الائتمانية * كما هو محدد في المادة ١ (١٥) في PDPL

أي بيانات شخصية تتعلق بطلب الفرد للحصول على تمويل من جهة تمويلية أو الحصول عليها، سواء كان لغرض شخصي أو عائلي، بما في ذلك أي بيانات تتعلق بقدرة هذا الفرد على الحصول على الديون وسدادها، والتاريخ الائتماني لذلك الشخص.

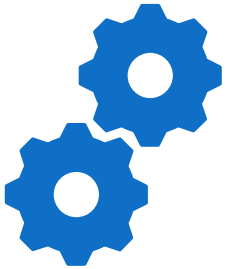
أصحاب البيانات* كما هو محدد في المادة ١ (١٦) في PDPL

"أصحاب البيانات" - أصحاب البيانات الفرد الذي تتعلق به البيانات الشخصية.

هم الأفراد الذين تتم معالجة بياناتهم الشخصية بواسطة متحكم البيانات أو معالج البيانات أو كليهما. على سبيل المثال:

- الموظفين
- الزبائن
- المتقدمون للوظائف
- البائعون والمقاولون
- زوار الموقع الألكتروني العام
- المساهمين

معالجة البيانات * المعرفة في المادة ١ (٥) في PDPL



"المعالجة" - أي عملية يتم تنفيذها على البيانات الشخصية بأي طريقة،

ملاحظة: حتى رؤية البيانات الشخصية، التي تؤدي إلى الاستخدام اللاحق في أي مكان، هي أيضا "معالجة".

- سواء كانت يدوية أو آلية ، بما في ذلك جمع البيانات وتسجيلها وحفظها وفهرستها وتنظيمها وتنسيقها وتخزينها وتعديلها وتحديثها ودمجها واسترجاعها واستخدامها والكشف عنها ونقلها ونشرها ومشاركتها وربطها وحظرها ومسحها وإتلافها.

المتحكم * كما هو محدد في المادة ١ (١٨) في PDPL

"**المتحكم** - " أي جهة عامة أو شخص طبيعي أو شخص قانوني خاص يحدد الغرض من معالجة البيانات الشخصية وطريقتها، سواء تمت معالجة البيانات من قبل المتحكم أو بواسطة المعالج. يطلق على المتحكم أيضا اسم مراقب البيانات في الصناعة.

الجهة العامة هي أي وزارة أو إدارة أو مؤسسة عامة أو هيئة عامة أو أي جهة عامة مستقلة في المملكة أو أي جهة تابعة لها.

الشخص القانوني الخاص هو أي شركة أو شركة مسجلة كجهة قانونية.

التزامات المتحكم

- يجب أن يتبنى المتحكم سياسة خصوصية البيانات ، ويجب أن تكون السياسة متاحة للأفراد لعرضها قبل جمع بياناتهم.

- إذا كان المتحكم يجمع البيانات مباشرة من مالك البيانات، فيجب عليه إبلاغه بما يلي:
  - الأساس القانوني لجمع البيانات
  - الغرض من جمع البيانات
  - التخزين وخيارات ممارسة حقوقهم
  - معلومات أولئك الذين يعالجونها
  - قرار نقل البيانات عبر الحدود
- يجب على متحكمين البيانات إعداد أنشطة معالجة البيانات الشخصية والاحتفاظ بها وتسجيلها.
- في حالة حدوث اختراق ، يجب إخطارهم على الفور للسلطة الإشرافية وأصحاب البيانات.

هل تُعتبر غرفة جدة جهة متحكّمة؟ (Controller)

إذا قاموا بمعالجة البيانات الشخصية على أي مما يلي:

- ✓ الموظفين وأفراد أسرهم.
- ✓ عملاء منتجاتهم
- ✓ الشركاء في الأعمال
- ✓ البائعون في الأعمال
- ✓زوار الموقع الإلكتروني العام لغرفة جدة

المعالج * كما هو محدد في المادة ١ (٥) في PDPL

"المعالج " أي جهة عامة أو شخص طبيعي أو شخص قانوني خاص **يقوم بمعالجة البيانات الشخصية لصالح المتحكم ونيابة عنه.**

يطلق على المعالج أيضا اسم معالج البيانات في الصناعة.

- معالجة البيانات الشخصية نيابة عن المتحكم
- يعمل بناء على تعليمات المتحكم
- تحكم محدود في البيانات

الأسس القانونية لمعالجة البيانات

- **الموافقه :** تم الحصول على موافقة واضحة وصريحة من صاحب البيانات لأغراض محددة. يجب أن تكون الموافقة مستنيرة وطوعية.
- **المصلحة المشروعة :** مصلحة ضرورية للمتحكم لمعالجة البيانات ، وضمان عدم انتهاكها لحقوق صاحب البيانات .
- **الالتزام القانوني :** المعالجة المطلوبة للامتثال للمتطلبات القانونية (مثل الضرائب وقوانين العمل) التي لا تتطلب موافقة.
- **الضرورة التعاقدية :** المعالجة ضرورية للوفاء بعقد مع صاحب البيانات أو لاتخاذ خطوات أولية قبل إبرام عقد (على سبيل المثال ، التوظيف والقروض).
- **المصلحة الحيوية** : المعالجة ضرورية لحماية حياة صاحب البيانات .
- **المصلحة العامة :** المعالجة ضرورية للمهام التي تخدم المصلحة العامة أو لممارسة السلطة الرسمية، ولا سيما ذات الصلة بالمبادرات الحكومية أو العامة.
- **الفائدة الفعلية :** المصلحة المعنوية أو المادية لصاحب البيانات المرتبطة بغرض معالجة البيانات ، وهي ضرورية لتحقيق هذه الاهتمام.

مبادئ معالجة البيانات

- تقليل البيانات
- تحديد الغرض
- الشرعية والشفافية
- النزاهة والسرية
- قيود التخزين
- الدقة
- المسائلة

حقوق صاحب البيانات

- الحق في الحصول على المعلومات
- حق الوصول
- الحق في تعديل البيانات الشخصية
- الحق في الحذف
- الحق في الاعتراض أو تقييد المعالجة

الاعفاءات * كما هو محدد في المادة ٢

لا تنطبق PDPL ولوائحها عندما يقوم الفرد بمعالجة البيانات الشخصية لأغراض شخصية أو عائلية بحتة.

ملاحظة:

- يشير الاستخدام الشخصي أو العائلي إلى معالجة البيانات داخل الدائرة الخاصة أو الاجتماعية للفرد ، مثل العائلة أو الأصدقاء المقربين.
- إذا تم نشر البيانات الشخصية للعامة أو مشاركتها مع أطراف ثالثة غير مصرح لها ، فلن تكون مؤهلة للاستخدام الشخصي أو العائلي.

نقل البيانات خارج المملكة العربية السعودية

أغراض النقل المسموح بها:

- الوفاء بالاتفاقيات المتعلقة بالمملكة.
- لخدمة مصالح المملكة.
- للوفاء بالالتزامات المتعلقة بصاحب البيانات.
- لأي أغراض أخرى منصوص عليها في اللائحة.

شروط النقل أو الإفصاح:

- يجب ألا يعرض الأمن القومي أو المصالح الحيوية للمملكة للخطر.
- يجب ضمان الحماية الكافية للبيانات الشخصية، بما يتفق مع معايير المملكة.
- يجب أن تقتصر عمليات النقل على الحد الأدنى من البيانات الضرورية.

الاستثناءات:

لا يجوز تطبيق هذه الشروط في حالات الضرورة القصوى، مثل:

- الحفاظ على حياة أو مصالح صاحب البيانات.
- الوقاية من الحالات الطبية أو تشخيصها أو علاجها.

الضمانات: الحماية الكافية، البنود التعاقدية القياسية (SCCs)، قواعد الشركة الملزمة، شهادة الاعتماد، الموافقة، الموافقة الصريحة من SDAIA

تقييم تأثير الخصوصية

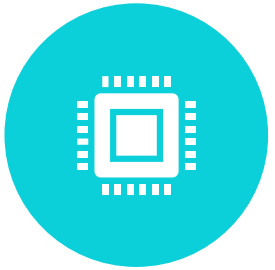
- يُستخدم تقييم تأثير الخصوصية لتقييم كيف يمكن لأنشطة معالجة البيانات الشخصية أن تؤثر على حقوق خصوصية الأفراد.
- يُحدّد التقييم ويحلل المخاطر المحتملة على الخصوصية ضمن عمليات معالجة البيانات المحددة.
- يساعد هذا التقييم في ضمان الامتثال لنظام حماية البيانات الشخصية من خلال تحديد الضوابط القانونية والتقنية والتنظيمية المناسبة.
- تكون نتيجة التقييم تقريرًا عن مخاطر الخصوصية يتضمن استراتيجيات تخفيف المخاطر وتوصيات قابلة للتنفيذ لتقليل المخاطر المحددة.

ROPA / PIA

الجانب	سجل أنشطة المعالجة (ROPA)	تقييم تأثير الخصوصية (PIA)
الغرض	الاحتفاظ بقائمة جرد لجميع أنشطة معالجة البيانات الشخصية داخل المؤسسة.	لتقييم تأثير أنشطة المعالجة على الخصوصية الفردية.
المتطلبات التنظيمية	مطلوب بموجب PDPL.	موصى به أو مطلوب لأي نشاط معالجة قد يكون له آثار على الخصوصية.
يركز	يوفر نظرة عامة تنظيمية على جميع أنشطة المعالجة.	يحلل مخاطر الخصوصية في سياقات معالجة بيانات محددة.
الناتج	سجل مركزي أو سجل لأنشطة المعالجة.	تقرير مخاطر الخصوصية مع توصيات قابلة للتنفيذ.

دورة حياة البيانات

تجميع المعلومات



الاستخدام / المعالجة

التخزين / التخلص

الإفصاح / الإنتقال

مسؤول حماية البيانات (DPO)

تنفيذي أو موظف داخل المنظمة أو مقاول خارجي للمتحكم.

يجب تعيين مسؤول حماية البيانات في السيناريوهات التالية:

- إذا كان المتحكم جهة عامة تعالج البيانات الشخصية على نطاق واسع.
- إذا كانت الأنشطة الأساسية للمتحكم تنطوي على مراقبة منتظمة ومنهجية لأصحاب البيانات.
- إذا كانت الأنشطة الأساسية تنطوي على معالجة البيانات الشخصية الحساسة أو البيانات المتعلقة بالإدانات والجرائم الجنائية.
- يجب على المتحكمين تعيين واحد على الأقل من موظفيهم ليكون مسؤولا عن تحقيق الامتثال للقانون.

مسؤوليات DPO :

- تأكد من الامتثال ل PDPL من قبل المتحكم.
- العمل كجهة اتصال للسلطة المختصة.
- الإشراف على تقييمات تأثير الخصوصية والحفاظ على الوثائق المناسبة.
- إخطار الجهة المختصة بأي اختراقات للبيانات الشخصية.
- تسهيل حقوق أصحاب البيانات ومعالجة طلباتهم أو شكاواهم.
- مراقبة وتحديث سجلات أنشطة معالجة البيانات الشخصية.
- تحديد الانتهاكات واقتراح الإجراءات التصحيحية.

إشعار اختراق البيانات

- **إشعار الجهة المختصة :**إشعار في غضون ٧٢ ساعة إذا كان الاختراق قد يضر بالبيانات الشخصية أو حقوق أصحاب البيانات.

- **يجب أن يتضمن الإشعار :**وصف الاختراق (الوقت والتاريخ والتفاصيل) والبيانات المتأثرة (الفئات وعدد اصحاب البيانات وأنواع البيانات) والمخاطر وتدابير التخفيف وخطوات الوقاية المستقبلية.

- **إشعار أصحاب البيانات (إن وجد):** أبلغهم دون تأخير إذا كان الاختراق قد يضر بحقوقهم. تقديم تفاصيل الاختراق والمخاطر والمشورة للحماية.

Q & A

غرفة جدة
JEDDAH CHAMBER
— 1946 —

كانو إليت
Kanoo Elite
Envision. Engage. Evolve.

شكرا لكم!