سياسة حماية البيانات والخصوصية

شركة انغوت للخدمات المالية ش. ذ. م. م.

تاريخ المراجعة: 09 أبريل 2026

انغوت للخدمات المالية ش.ذ.م.م.

info@ingot.io info@ingot.io www.ingot.io

مكتب 1، مبنى رقم 3، إعمار سكوير، داون تاون، دبي، الإمارات العربية المتحدة.

صندوق بريد:191741

1. المُقدّمة:

قانون حماية البيانات الشخصية

يُشكّل قانون حماية البيانات الشخصية، الصادر بموجب المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، إطاراً متكاملاً بهدف ضمان سرية المعلومات وحماية خصوصية الأفراد في دولة الإمارات العربية المتحدة. كما يضع هذا القانون أسساً واضحة وسليمة لحوكمة إدارة البيانات وحمايتها، ويُحدّد حقوق وواجبات جميع الأطراف المعنيّة.

وفيما يلي مُلخّص لأبرز أحكام وبنود هذا القانون:

- تسري أحكام القانون على معالجة البيانات الشخصية، سواء كلياً أو جزئياً، عبر الأنظمة الإلكترونية داخل الدولة أو خارجها.
- يُحدّد القانون ضوابط معالجة البيانات الشخصية، والالتزامات العامة للشركات التي تحتفظ بها بهدف حمايتها والحفاظ على سريتها وخصوصيتها. كما يحظر معالجة البيانات الشخصية دون موافقة صاحبها، باستثناء بعض الحالات التي تكون فيها المعالجة ضرورية لحماية المصلحة العامة أو لتنفيذ أي من الإجراءات والحقوق القانونية.
- يمنح القانون صاحب البيانات الحق في طلب تصحيح البيانات الشخصية غير الدقيقة/غير الصحيحة، وطلب الحد من معالجتها أو إيقافها.
- يُحدّد القانون متطلبات نقل البيانات الشخصية ومشاركتها عبر الحدود (خارجياً) لأغراض المعالجة.

تشريعات أخرى ذات صلة:

تشمل القوانين الأخرى المتعلقة بحماية البيانات والخصوصية ما يلي:

- **قانون حماية المستهلك**

ينص القانون الاتحادي رقم (15) لسنة 2020 بشأن حماية المستهلك على حماية جميع حقوق المستهلك، بما في ذلك بياناته، ويحظر على مُزوّدي الخدمات استخدامها لأغراض تسويقية.

- **حماية البيانات والخصوصية عبر الإنترنت**

سياسة إدارة الوصول إلى الإنترنت (IAM)

تتولى هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA) تطبيق هذه السياسة في دولة الإمارات العربية المتحدة بالتنسيق مع المجلس الوطني للإعلام وشركتي "اتصالات" و"دو"، وهما شركتان لتزويد خدمة الإنترنت ومرخصتان في الدولة. وبموجب هذه السياسة، يُمكن الإبلاغ عن أي محتوى إلكتروني يُستخدم لانتحال الشخصية أو التحايل أو التصيّد الإلكتروني أو لانتهاك الخصوصية، إلى شركتي "اتصالات" و"دو" لإزالته.

- **قانون المعاملات الإلكترونية وخدمات الثقة**

يُنظّم هذا القانون كل ما يتعلّق بصحة المستندات الإلكترونية، ويُعزّز القيمة القانونية للتوقيع الرقمي ومستوى أمانه، ويتضمن البنود والأحكام الخاصة بالمعاملات الإلكترونية، وكيفية تخزين المستندات الإلكترونية وحفظها وإرسالها واستلامها لضمان صحتها. كما يُحدّد متطلبات الترخيص لمُزوّدي خدمات الثقة المرخّص لهم رسمياً بإنشاء وتوثيق وحفظ التوقيعات الإلكترونية والأختام الإلكترونية والشهادات الرقمية.

- **دستور دولة الإمارات العربية المتحدة**

تنص المادة (31) من دستور دولة الإمارات العربية المتحدة على حرية التواصل عبر البريد أو البرقيّة أو أي وسيلة اتصال أخرى، وتضمن سرية هذه الاتصالات بموجب القانون.

- **حماية حقوق الملكية وبراءات الاختراع والعلامات التجارية**

بصفتها شركة خاضعة لتنظيم هيئة سوق المال ("CMA")، وتعمل في دولة الإمارات العربية المتحدة، تلتزم شركة انغوت للخدمات المالية ش. ذ. م. م. ("الشركة") بحماية خصوصية وسرية وأمن بيانات عملائها. وتُوضح سياسة البيانات هذه التدابير

التي نتخذها لضمان حماية البيانات الشخصية المتعلقة بعملائنا وفقاً لقانون حماية البيانات الشخصية والتشريعات الأخرى ذات الصلة.

2. التعريفات

"أغراض العمل": هي الأغراض التي يجوز لنا أن نستخدم البيانات الشخصية من أجلها، وتشمل: شؤون الموظفين، والشؤون الإدارية، والشؤون المالية، والشؤون التنظيمية، والرواتب، وتطوير الأعمال.

تشمل أغراض العمل ما يلي:

- الامتثال لالتزاماتنا القانونية والتنظيمية وتلك المتعلقة بحوكمة الشركات، إلى جانب الالتزام بأفضل الممارسات.
- جمع المعلومات كجزء من التحقيقات التي تُجريها الهيئات التنظيمية أو فيما يتعلق بالإجراءات أو الطلبات القانونية.
- أسباب تشغيلية مثل تسجيل المعاملات، والتدريب، ومُراقبة الجودة لضمان سرية المعلومات الحساسة الخاصة بأعمال الشركة، والتحقّق الأمني، وتقييم الجدارة الائتمانية.
- التحقيق في الشكاوى.
- التحقّق من المراجع، وضمان ممارسات العمل الآمنة، ومراقبة وإدارة وصول الموظفين إلى الأنظمة والمرافق، ومتابعة غيابات الموظفين، والتقييمات، والشؤون المتعلقة بالإدارة.
- مراقبة سلوك الموظفين، والمسائل التأديبية.
- تسويق أعمالنا.
- تحسين خدماتنا.

"صاحب البيانات": هو شخص طبيعي؛ تخصّه البيانات الشخصية.

"الموافقة": هي الإذن الذي يمنحه صاحب البيانات لطرف ثالث ليقوم بمعالجة بياناته الشخصية، شريطة أن تُشير هذه الموافقة، وفقاً للمرسوم بقانون اتحادي 45 بشأن قانون حماية البيانات الشخصية، بطريقة مُحدّدة وواضحة لا لُبْسَ فيها، إلى أنه يقبل معالجة بياناته الشخصية من خلال بيان أو إجراء إيجابي واضح.

"البيانات الشخصية": هي أي بيانات تتعلق بشخص طبيعي مُحدّد أو بشخص طبيعي يُمكن التعرّف عليه بشكل مباشر أو غير مباشر من خلال ربط البيانات، أو باستخدام عناصر تعريفية مثل اسمه، أو صوته، أو صورته، أو رقم هويته، أو مُعرّفه الإلكتروني، أو موقعه الجغرافي، أو من خلال سمة أو أكثر من سماته البدنية، أو الفيزيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية. وتشمل البيانات الشخصية الحساسة والبيانات البيومترية.

"المعالجة": هي أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية باستخدام أي وسيلة إلكترونية، بما في ذلك التعاملات وغيرها. تشمل هذه المعالجة جمع البيانات الشخصية وتخزينها وتسجيلها وتنظيمها وضبطها وتعديلها وتداولها وتغييرها واسترجاعها وتبادلها ومشاركتها واستخدامها وتوصيفها والإفصاح عنها عن طريق نشرها أو إرسالها أو توزيعها أو توفيرها أو تنسيقها أو دمجها أو طلب الحد من معالجتها أو حجبها أو محوها أو إتلافها أو إنشاء نُسَخ منها.

"البيانات الشخصية الحساسة": هي أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة شخص طبيعي، أو أصله العرقي، أو آرائه السياسية أو الفلسفية، أو معتقداته الدينية، أو سِجّله الجنائي، أو بياناته البيومترية، أو أي بيانات تتعلق بصحة هذا الشخص وحالته البدنية أو النفسية أو العقلية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بالبنود والأحكام ذات الصلة بتقديم خدمات الرعاية الصحية له والتي تكشف عن حالته الصحية.

"المكتب": هو الهيئة الوطنية المسؤولة عن حماية البيانات. أما الجهة الرقابية على الشركة فهي مكتب بيانات دولة الإمارات العربية المتحدة، الذي تم إنشاؤه بموجب المرسوم بقانون اتحادي رقم (45) لسنة 2021، المذكور أعلاه.

3. نطاق السياسة

تنطبق هذه السياسة على الموظفين، ويجب عليهم الإلمام بها والامتثال لأحكامها.

تُوضّح هذه السياسة الإجراءات التي تتبعها الشركة لحماية البيانات الشخصية، وتضمن فهم الموظفين للقواعد والقوانين المتعلقة باستخدام البيانات الشخصية التي يُمكنهم الوصول إليها أثناء عملهم. وتُلزم هذه السياسة على وجه الخصوص الموظفين باستشارة مسؤول حماية البيانات الذي تم تعيينه قبل البدء بأي إجراء جديد ومهم لمعالجة البيانات، وذلك لضمان اتخاذ جميع خطوات وتدابير الامتثال اللازمة.
تحتفظ الشركة بحقها في إضافة أي ملحق أو تعديل هذه السياسة بسياسات وإرشادات إضافية من حين لآخر، إذا لزم الأمر. وسيتم تعميم أي سياسة جديدة أو مُعدّلة على الموظفين قبل اعتمادها.
يتحمّل مسؤول حماية البيانات الذي تم تعيينه المسؤوليةَ الكاملة عن تطبيق هذه السياسة بشكل يومي.

4. ضوابط معالجة البيانات الشخصية

تتم معالجة البيانات وفقاً للضوابط التالية المنصوص عليها في القانون:

- إجراء المعالجة بطريقة عادلة وشفّافة وقانونية.
- جمع البيانات الشخصية لغرض مُحدّد وواضح، وعدم القيام بمعالجتها لاحقاً بطريقة تتعارض مع هذا الغرض. ومع ذلك، يجوز معالجتها إذا كان الغرض مُشابهاً أو قريباً من الغرض الذي جُمعت من أجله.
- التأكد من أن البيانات الشخصية كافية ومُقتصرة على ما هو ضروري وفقاً للغرض الذي يتم إجراء المعالجة من أجله.
- اتخاذ التدابير اللازمة لضمان حذف البيانات الشخصية غير الصحيحة أو القيام بتصحيحها.
- حفظ البيانات الشخصية بشكل آمن، بما في ذلك حمايتها من أي انتهاك أو اختراق أو معالجة غير قانونية أو غير مُصرّح بها، وذلك من خلال تطوير واستخدام تدابير وإجراءات تقنية وتنظيمية مُناسبة وفقاً للقوانين والتشريعات السارية في هذا الشأن.
- عدم حفظ البيانات الشخصية بعد انتهاء الغرض من معالجتها. ويجوز الاحتفاظ بها إذا تم إخفاء هوية صاحب البيانات باستخدام "آلية إخفاء الهوية".
- أي ضوابط أخرى منصوص عليها في اللوائح التنفيذية لهذا المرسوم بموجب القانون.

5. جمع ومعالجة البيانات الشخصية

نقوم بجمع ومعالجة البيانات الشخصية فقط بالقدر اللازم لتقديم خدماتنا والامتثال للمتطلبات القانونية. يتم جمع البيانات الشخصية مباشرةً من العميل أو من جهات خارجية (أطراف ثالثة) مُصرَّح لها. علاوة على ذلك، يجب أن تحتفظ الشركة دائماً بموافقة صريحة وواضحة ومُحدّدة ومُحدّثة من العميل على معالجة بياناته لغرض مُحدّد.

المعلومات التي يُقدّمها العميل للشركة

- بيانات الهوية، مثل: الاسم الأول، واسم العائلة، وتاريخ الميلاد، والجنسية.
- معلومات التواصل، مثل: العنوان، والبريد الإلكتروني، ورقم الموبايل.
- وثائق ومستندات إثبات الهوية (مثل: جواز السفر)، والصور، والتسجيلات الصوتية، والفيديوهات، وأي معلومات أخرى لأغراض التحقّق من الهوية بهدف إثبات أهلية العميل لاستخدام خدمات الشركة.
- تفاصيل الحساب البنكي، أو بطاقات السحب الآلي الفوري، أو البطاقات الائتمانية.
- البيانات التي يختار العميل تقديمها للشركة للحصول على خدمات مُحدّدة، مثل عنوان الاستلام أو عنوان العمل أثناء تقديم طلب للحصول على خدماتنا المخصّصة لأغراض الأعمال.
- المعلومات التي يتم تقديمها من خلال التواصل مع الشركة، سواءً عبر الهاتف، أو البريد الإلكتروني، أو الإنترنت، أو غير ذلك.
- البيانات والمحتوى الذي يُقدّمه العميل عند المشاركة في المناقشات أو الاستبيانات أو العروض الترويجية عبر الإنترنت، بما في ذلك ما تنشره الشركة على صفحاتها على مواقع التواصل الاجتماعي ومنصاتها الرقمية.
- صورة (في حال تحميلها فقط).
- المعلومات التي نحصل عليها من العميل أو نستخلصها عنه.
- البيانات الشخصية المستخرجة من المستندات التعريفية.
- معلومات حول الخدمات التي يستخدمها العميل.

- معلومات حول زيارة العميل، بما في ذلك الروابط التي قام بالنقر عليها، أو التي وصل إليها عبر الموقع أو أثناء الاستخدام (بما في ذلك التاريخ والوقت)، والخدمات التي قام بالاطّلاع عليها أو البحث عنها، ووقت استجابة الصفحات، وأخطاء التنزيل، ومدة الزيارات لصفحات مُعيّنة، وتفاصيل التفاعل مع الصفحة (مثل عدد النقرات وعدد مرّات التصفّح)، والطرق المستخدمة للخروج من الصفحة، والرموز/العلامات المستخدمة لتحديد اللغات البشرية.
- المعلومات التقنية، بما في ذلك عنوان بروتوكول الإنترنت (IP) المستخدم للاتصال بالإنترنت، ومعلومات تسجيل الدخول، ونوع المتصفح وإصداره، وإعدادات النطاق الزمني، ونظام التشغيل والمنصة، ونوع الجهاز، ورقم تعريف الجهاز (على سبيل المثال، رقم IMEI الخاص بالجهاز، وعنوان MAC الخاص بواجهة الشبكة اللاسلكية للجهاز)، ومعلومات شبكة الهاتف المحمول، وغير ذلك.
- ملفات تعريف الارتباط والتقنيات المشابهة التي تستخدمها الشركة للتعرّف على العميل، واسترجاع تفضيلاته، وتخصيص المحتوى الذي تُقدّمه الشركة.
- معلومات تقييم المخاطر، مثل أنماط المعاملات ومعلومات الاكتتاب.
- بيانات التحقيقات والمعلومات العامة، مثل عمليات التحقق كما في العناية الواجبة، والعقوبات، ومكافحة غسل الأموال.
- المعلومات التي نحتاجها لدعم التزاماتنا التنظيمية، مثل تلك المتعلقة بتفاصيل المعاملات، والكشف عن أي نشاط مشبوه أو غير معتاد.

نقوم بمعالجة البيانات الشخصية للأغراض التالية:

- التحقق من الهوية ومكافحة غسل الأموال.
- تقديم وإدارة الخدمات المالية.
- منع محاولات الاحتيال وكشفها.
- الامتثال للمتطلبات القانونية والتنظيمية.

لا نستخدم البيانات الشخصية لأي غرض آخر غير المذكور أعلاه إلا بعد الحصول على موافقة صريحة وواضحة من العميل.

6. مشاركة البيانات الشخصية

قد نقوم بمشاركة البيانات الشخصية مع الجهات الخارجية التالية:

- مُزوّدو الخدمات المالية.
- هيئات مكافحة الاحتيال.
- الهيئات التنظيمية والإشرافية.

كما قد نُشارك البيانات الشخصية مع جهات خارجية أخرى بموافقة صريحة من العميل أو وفقاً لما يقتضيه القانون. ويُمكن أيضاً الإفصاح عن البيانات في الحالات التالية:

- إذا كان الإفصاح ضرورياً بشكل منطقي ومعقول لتقديم خدمة مالية مُحدّدة للعميل.
- إذا لم تعد المعلومات سرية.
- إذا تم طلب الإفصاح عنها من قبل جهات قضائية أو رقابية في الدولة، مثل هيئة سوق المال.

7. التدابير الأمنية

لقد قمنا بتطبيق تدابير تقنية وتنظيمية مناسبة لضمان أمن البيانات الشخصية. ويشمل ذلك ما يلي:

- ضبط الوصول إلى البيانات الشخصية.
- تشفير البيانات أثناء نقلها.
- تخزين البيانات الشخصية بشكل آمن.
- تدقيق أمني دوري وتقييم المخاطر.

في حال تخزين البيانات على ورق مطبوع، يجب حفظها في مكان آمن بعيداً عن مُتناول الأشخاص غير المُصرّح لهم بالوصول إليها. ويجب إتلاف البيانات المطبوعة عند انتهاء الحاجة إليها. أما البيانات المُخزّنة على جهاز الحاسوب، فيجب حمايتها بكلمات مرور قوية يتم تغييرها بانتظام. وعلى جميع الموظفين استخدام برنامج مخصصة لإدارة كلمات المرور سواء لإنشائها أو تخزينها. ويجب تشفير البيانات المُخزّنة على الأقراص المدمجة أو الفلاش أو حمايتها بكلمة مرور وحفظها في مكان آمن عند عدم استخدامها. وعلى مسؤول حماية البيانات الموافقة على أي خدمة سحابية تُستخدم لتخزين البيانات. ويجب العمل على حفظ الخادم الذي يحتوي على بيانات شخصية في موقع آمن، وأن يتم حمايته عبر برامج آمنة. ويجب أن يتم نسخ البيانات الاحتياطية بانتظام وفقاً لإجراءات النسخ الاحتياطي المعتمدة في الشركة، ولا يجوز حفظها مباشرةً على الأجهزة المحمولة مثل أجهزة الكمبيوتر المحمولة أو الأجهزة اللوحية أو الهواتف الذكية. وينبغي كذلك اتخاذ جميع التدابير التقنية الممكنة للحفاظ على أمان البيانات.

8. الاحتفاظ بالبيانات الشخصية

نحتفظ بالبيانات الشخصية في حال كان ذلك ضرورياً للوفاء بالتزاماتنا القانونية والتنظيمية أو للأغراض التي جُمعت من أجلها. وبمُجرّد انتهاء الحاجة إلى هذه البيانات، فإننا نقوم بحذفها أو إخفاء هوية صاحبها بشكل آمن. وتختلف مدة الاحتفاظ بالبيانات باختلاف ظروف كل حالة، مع مراعاة الأسباب التي جُمعت من أجلها، على أن تُحدَّد بما يتوافق مع إرشادات الاحتفاظ بالبيانات. وبموجب اللوائح المعمول بها، تحتفظ الشركة بسجّلات تتضمن بيانات العميل الشخصية، ومعلومات التداول، ومستندات فتح الحساب، والمراسلات، وأي شيء آخر يتعلق بالعميل، لمدة لا تقل عن خمس سنوات بعد انتهاء العلاقة التعاقدية معه.

9. حقوق أصحاب البيانات

يحق للعملاء ما يلي:

- الوصول إلى بياناتهم الشخصية.
- تصحيح أي أخطاء في بياناتهم الشخصية.
- طلب حذف بياناتهم الشخصية.
- الاعتراض على معالجة بياناتهم الشخصية.
- طلب الحد من معالجة بياناتهم الشخصية.
- الحصول على نسخة من بياناتهم الشخصية بشكل مُنظّم ومُتعارف عليه وقابل للقراءة والمعالجة آلياً.

سنقوم بالرد على جميع الطلبات خلال مدة لا تتجاوز شهراً واحداً، وبتزويد المعلومات مجّاناً في حال كان الطلب مبنيّاً على أساس واضح ولا يتجاوز الحد المعقول والمنطقي.

10. الأطراف الثالثة (الخارجية)

يجب أن يكون لدى الشركة عقود مكتوبة سارية مع أي جهات خارجية مسؤولة عن معالجة البيانات أو/و التحكم بها، والتي تعتزم إبرامَ اتفاقية معها. يجب أن تتضمن الاتفاقية بنوداً مُحدّدة تُوضّح المسؤوليات والالتزامات والأعباء المترتبة على كل من الشركة والجهات الخارجية (الأطراف الثالثة). كما ينبغي على الشركة تعيين جهات (أطراف) تقوم بمعالجة البيانات بحيث تكون قادرة على تقديم ضمانات كافية بموجب القانون، وبشكل يكفل احترام حقوق أصحاب البيانات وحمايتها.

11. مسؤول حماية البيانات

المهام المترتبة على مسؤول حماية البيانات

- إطلاع مجلس الإدارة على مسؤوليات حماية البيانات والمخاطر والقضايا المتعلقة بها.
- مراجعة جميع إجراءات وسياسات حماية البيانات بشكل منتظم.
- تنظيم دورات تدريبية وتقديم الاستشارات حول حماية البيانات لجميع الموظفين والأشخاص الذين تشملهم هذه السياسة.
- الإجابة على استفسارات الموظفين وأعضاء مجلس الإدارة والجهات المعنيّة الأخرى بشأن أي سؤال عن حماية البيانات.
- الرد على استفسارات الأفراد، كالعملاء والموظفين، الراغبين في معرفة البيانات التي تحتفظ بها الشركة عنهم.
- التحقّق من جودة وصحة الإجراءات المطبّقة في الشركة.
- استلام الطلبات والشكاوى المتعلقة بالبيانات الشخصية وفقاً لأحكام المرسوم ولائحته التنظيمية التنفيذية.

- تقديم الاستشارات المتخصصة بشأن إجراءات التقييم والفحص الدوري لأنظمة حماية البيانات الشخصية وأنظمة منع الاختراق في الشركة، وتوثيق نتائج هذا التقييم، وتقديم التوصيات المناسبة في هذا الشأن، بما في ذلك إجراءات تقييم المخاطر.
- أي مهام أو صلاحيات أخرى يتم تحديدها وفقاً للائحة التنظيمية التنفيذية ذات الصلة بالمرسوم.

يلتزم مسؤول حماية البيانات بالحفاظ على سرية المعلومات والبيانات التي يتلقاها أثناء قيامه بمهامه وممارسته لصلاحياته، وذلك وفقاً لأحكام المرسوم ولائحته التنظيمية التنفيذية، وللتشريعات السارية في الدولة.

لقد قمنا بتعيين مسؤول لحماية البيانات (DPO) للإشراف على ممارساتنا وإجراءاتنا المتبعة في مجال حماية البيانات. ويُمكن التواصل معه عبر البريد الإلكتروني التالي: info@ingot.ae

عند تقييم التدابير التقنية المناسبة، سيقوم مسؤول حماية البيانات/المسؤول عن الامتثال للائحة التنظيمية العامة لحماية البيانات (GDPR)بأخذ النقاط التالية في الاعتبار:

- حماية كلمة المرور.
- تفعيل القفل التلقائي للأجهزة عند بقائها دون استخدام لفترة معينة.
- إلغاء صلاحيات الوصول إلى الفلاش وغيرها من وسائل التخزين.
- فحص الفيروسات من خلال برامج الحماية المخصّصة لهذا الغرض.
- تحديد صلاحيات الوصول إلى البيانات وفقاً للمناصب الوظيفية؛ بما في ذلك تلك الممنوحة للكوادر التي تعمل في الشركة بشكل مؤقت.
- تشفير الأجهزة التي يُغادر أصحابها الشركة، مثل أجهزة الحاسوب المحمولة.
- استعادة إمكانية الوصول إلى البيانات الشخصية في الوقت المناسب في حال وقوع أي حادث مادي أو تقني.
- إجراء اختبارات وتقييمات دورية لقياس فعالية التدابير التقنية والتنظيمية المتبعة بهدف ضمان أمان عمليات المعالجة.
- الحفاظ على أمن الشبكات المحلية والشبكات واسعة النطاق.
- استخدام تقنيات تعزيز الخصوصية مثل إخفاء الهوية والأسماء المستعارة.
- تحديد معايير الأمن الدولية المناسبة لشركة انغوت للخدمات المالية ش. ذ. م. م.

عند تقييم التدابير التنظيمية المناسبة، سيأخذ مسؤول حماية البيانات في الاعتبار ما يلي:

- تحديد مستويات التدريب المناسبة لجميع أقسام شركة انغوت للخدمات المالية ش. ذ. م. م.
- وضع التدابير التي تُراعي موثوقية الموظفين (مثل التوصيات وغيرها).
- إدراج حماية البيانات في عقود العمل.
- اتخاذ إجراءات تأديبية في حال حدوث انتهاكات للبيانات.
- مراقبة التزام الموظفين بمعايير الأمان ذات الصلة.
- وضع ضوابط تتعلق بالوصول المادي إلى السجّلات الإلكترونية والورقية.
- اعتماد سياسة المكتب النظيف.
- تخزين البيانات الورقية في خزائن مُغلقة بإحكام ومُقاومة للحريق.
- الحدّ من استخدام أجهزة الحاسوب المحمولة الخاصة بالشركة خارج مكان العمل.
- الحدّ من قيام الموظفين باستخدام أجهزتهم الشخصية في مكان العمل.
- اعتماد قواعد واضحة بشأن كلمات المرور.
- إجراء عمليات نسخ احتياطي بشكل منتظم للبيانات الشخصية وحفظها خارج الشركة؛ في مواقع آمنة.
- اتخاذ تدابير أمنية مناسبة عند نقل البيانات خارج دولة الإمارات العربية المتحدة، وفرض التزامات تعاقدية على الجهات التي يتم تصدير البيانات إليها.

تم اختيار هذه الضوابط استناداً إلى المخاطر المُحدّدة التي تُهدّد البيانات الشخصية، ووفقاً لاحتماليات وقوع ضرر أو أذى للأفراد الذين تتم معالجة بياناتهم.

12. التدريب

سيتم توفير تدريب كافٍ على أحكام لائحة حماية البيانات لجميع الموظفين، بما يتناسب مع وظائفهم ومناصبهم. وفي حال تم تغيير صلاحيات الموظف أو منصبه، فإنه يتحمّل مسؤولية طلب تدريب جديد في مجال حماية البيانات بشكل ينسجم مع وظيفته أو مسؤولياته الجديدة.

13. مخاطر حماية البيانات

تُساعد هذه السياسة في حماية شركة انغوت للخدمات المالية ش. ذ. م. م. من أي مخاطر محتملة ذات علاقة بأمن البيانات؛ بما في ذلك:

- **الإخلال بالسرية:** مثل معالجة المعلومات بشكل غير لائق وبأسلوب غير مناسب.
- **الإضرار بالسمعة:** على سبيل المثال، قد تتعرض الشركة لأضرار مادية أو معنوية إذا تمكن المتسللون أو المخترقون من الوصول إلى بيانات حساسة.

14. المراجعة الدورية

تُجرى تقييمات سياسات حماية البيانات الخاصة بالشركة ضمن عملية المراجعة السنوية، أو خلال الاجتماعات الشهرية للجنة الحوكمة والمخاطر، وذلك لضمان التزام الشركة بالمعايير اللازمة.
وتُراجع هذه السياسة سنوياً أو بحسب الحاجة. وتُعتمد أي مراجعة مبدئياً من قِبل لجنة الحوكمة والمخاطر والامتثال. ويتم التشاور مع جميع الأطراف المعنية وصُنّاع القرار قبل الحصول على الموافقة النهائية من مجلس الإدارة.

الخلاصة

نحن ملتزمون بحماية البيانات الشخصية لعملائنا، وسنُواصل مراجعة وتحسين إجراءات حماية البيانات لدينا بما يتماشى مع أحدث المتطلبات القانونية والتنظيمية.