



سياسة حماية البيانات الشخصية

مدير دائرة الامتثال

سفيان القيمري

المدير العام

محمد علي مسلم

رئيس قسم الشبكات وأمن المعلومات

رجائي ابوالهوى

2026/4/20	تاريخ تطبيق السياسة
2026/4/28	تاريخ الاعتماد
	تاريخ التعديل

الإسناد

تم إعداد سياسة حماية البيانات الشخصية وفقاً لقانون حماية البيانات الشخصية رقم (24) لسنة 2023.

مقدمة

في إطار التزامها بأعلى معايير الخصوصية وأمن المعلومات، تُولي شركة المنارة الإسلامية للتأمين أهمية قصوى لحماية البيانات الشخصية لعملائها وموظفيها وجميع الأطراف المتعاملة معها وبصفتنا شركة تأمين، فإننا نتعامل مع معلومات حساسة تتعلق بالأفراد، ونلتزم بجمعها واستخدامها ومعالجتها بما يتوافق مع الأنظمة والتشريعات المعمول بها

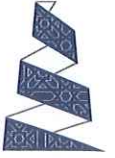
الغرض من السياسة

تهدف هذه السياسة إلى وضع إطار واضح ومنظم لحماية البيانات الشخصية التي تجمعها أو تعالجها شركة المنارة الإسلامية للتأمين سواء كانت هذه البيانات تخص العملاء أو الموظفين أو أي أطراف أخرى يتم التعامل معها وتهدف السياسة إلى ضمان التزام الشركة بجميع القوانين والأنظمة المحلية والدولية ذات الصلة بحماية الخصوصية، ولا سيما في ما يتعلق بالمعلومات الحساسة التي يتم جمعها في سياق تقديم خدمات التأمين.

كما تسعى هذه السياسة إلى تعزيز مبادئ الشفافية والمساءلة، وضمان استخدام البيانات الشخصية فقط للأغراض المشروعة والضرورية، مع اتخاذ التدابير الفنية والتنظيمية المناسبة لحمايتها من الوصول أو الاستخدام أو الإفشاء غير المصرح به، بما يحقق الثقة المتبادلة بين الشركة وعملائها ويحافظ على سمعة الشركة ومصداقيتها في السوق.

نطاق التطبيق

تنطبق سياسة حماية البيانات الشخصية في شركة المنارة الإسلامية للتأمين على جميع الأنشطة والعمليات التي يتم من خلالها جمع ومعالجة وتخزين ونقل وحذف البيانات الشخصية المتعلقة بالأطراف التالية :



1. العملاء (المؤمن لهم):
وتشمل جميع بياناتهم الشخصية والمالية والصحية التي يتم جمعها لأغراض تقديم الخدمات والمنتجات التأمينية .
2. الموظفين والمتعاقدين:
وتشمل بيانات التوظيف، الرواتب، وتفاصيل الاتصال الخاصة بالعاملين داخل الشركة أو المتعاقدين الخارجيين.
3. الوكلاء والمستشارين وشركاء الأعمال:
وتشمل البيانات التي يتم جمعها ضمن إطار العلاقة التعاقدية أو التشغيلية.
4. الأنظمة والتطبيقات:
تنطبق السياسة على جميع قواعد البيانات، الأنظمة الإلكترونية، التطبيقات، البريد الإلكتروني، وسائر الوسائط التي تُستخدم لمعالجة البيانات الشخصية داخل الشركة.
5. الأنشطة والعمليات:
تنطبق السياسة على كل من العمليات اليدوية والإلكترونية التي تمارسها الشركة:
 - إصدار وثائق التأمين
 - معالجة المطالبات
 - التحقق من الهوية
 - التسويق وخدمة العملاء
 - إدارة المخاطر والامتثال
 - إدارة الموارد البشرية

معالجة البيانات

تنص المادة الرابعة من قانون حماية البيانات الشخصية على أن معالجة البيانات الشخصية مسموح بها فقط بموافقة مسبقة صريحة من صاحب البيانات حيث تم اعتماد نموذج موقع من العميل يسمح بالاستعلام ومعالجة بياناته الشخصية حيث تلتزم الشركة بالموافقة المسبقة من العميل وتلتزم بالاستثناءات التي نص عليها القانون بما يلي :

باستثناء ذلك، يسمح القانون بمعالجة البيانات دون موافقة مسبقة في الحالات التالية:

- تقسم معالجة البيانات حسب قانون حماية البيانات الشخصية الى مايلي:-



1. بيانات الشخص الطبيعي ولا يجوز معالجتها إلا بعد الحصول على موافقة مسبقة للشخص المعني أو في الأحوال المصرح بها قانوناً وتكون الموافقة بشكل صريح وموثق خطياً أو إلكترونياً ومحددة المدة والعرض، يجتمع الشخص المعني بالحقوق المنصوص عليها في المادة (4) فقرة (ب) لقانون حماية البيانات الشخصية
2. معالجة بيانات الشخص المعني دون الحصول على الموافقة المسبقة أو إعلام الشخص المعني.
3. إذا كانت المعالجة تنفذ بواسطة جهة عامة مختصة ضمن نطاق مهامها الرسمية، أو بواسطة جهات متعاقدة معها وفق شروط واضحة في العقد.
4. لأغراض طبية وقائية أو تشخيصية أو تقديم رعاية صحية من جهة مرخص لها.
5. إذا كانت ضرورية لحماية حياة الشخص المعني أو مصالحه الحيوية.
6. لمنع أو كشف جريمة، أو متابعة الجرائم عبر جهة مختصة.
7. إذا كانت مطلوبة أو مصرح بها بموجب قانون أو بموجب قرار من محكمة مختصة.
8. لأداء الجهات الخاضعة لرقابة البنك المركزي الأردني لمهامها، بما فيها تبادل البيانات داخل الأردن أو خارجه.
9. إذا كانت وفق أحكام النظام الصادر بموجب هذا القانون.
10. لأغراض البحث العلمي أو التاريخي، بشرط عدم اتخاذ أي إجراء أو قرار مرتبط بشخص محدد.
11. لأغراض إحصائية، أو لمتطلبات الأمن الوطني، أو لتحقيق مصلحة عامة.
12. إذا كانت البيانات منشورة طوعاً من قبل الشخص المعني.

الأمن والتنظيم الداخلي

تلتزم الشركة باتخاذ جميع التدابير الفنية والتنظيمية المناسبة لضمان حماية البيانات الشخصية من الوصول غير المصرح به، أو فقدان أو التعديل أو الكشف أو الإتلاف، سواء كانت هذه البيانات محفوظة إلكترونياً أو ورقياً.

ولتحقيق ذلك تعتمد الشركة المبادئ التالية:

1. تعيين مسؤول حماية البيانات (DPO)
تم تعيين مسؤول لحماية البيانات والإشراف على تطبيق السياسة وضمان الامتثال لقانون حماية البيانات الشخصية.



2. إجراءات الوصول المقيد:
يُسمح فقط للموظفين المصرح لهم، وبما يتوافق مع طبيعة عملهم بالوصول إلى البيانات الشخصية ويتم استخدام أنظمة تحقق ثنائية (2FA) وكلمات مرور مشفرة لحماية الدخول.
3. التدريب والتوعية:
تم عمل برامج تدريب دورية لجميع الموظفين حول أهمية حماية البيانات والإجراءات الوقائية والتزاماتهم القانونية والأخلاقية تجاه خصوصية العملاء والمستفيدين.
4. تقييم المخاطر ومراجعة الأمان:
تقوم إدارة تقنية المعلومات بتنفيذ اختبارات دورية لتقييم نقاط الضعف الأمنية (Security Risk Assessments)، مع اتخاذ إجراءات تصحيحية فورية حال اكتشاف أي خلل.
5. توثيق المعالجة والسجلات:
يتم الاحتفاظ بسجلات موثقة لجميع عمليات معالجة البيانات بما يشمل طبيعة البيانات الغرض من معالجتها و الأطراف المعنية وأي عمليات نقل أو مشاركة تمت.
6. سياسات النسخ الاحتياطي والاسترداد:
تُطبق أنظمة نسخ احتياطي منتظمة لضمان استرداد البيانات عند الحاجة، خاصة في حالات الكوارث أو الأعطال التقنية.
7. الإخطار بالاختراقات:
في حال حدوث خرق أمني يُحتمل أن يؤثر على الأفراد تلتزم الشركة بإخطار الجهات التنظيمية وصاحب البيانات خلال المدة القانونية المحددة مع توضيح طبيعة الخرق والإجراءات التصحيحية المتخذة.

مراجعة وتحديث السياسة

تلتزم الشركة بمراجعة وتحديث سياسة حماية البيانات الشخصية بشكل دوري لضمان توافقها مع القوانين والتشريعات النافذة في المملكة الأردنية الهاشمية وعلى رأسها قانون حماية البيانات الشخصية رقم (24) لسنة 2023 وأي تعليمات أو أنظمة تصدر بمقتضاه.



تُجرى مراجعة هذه السياسة مرة واحدة على الأقل سنوياً أو فور حدوث أي من الحالات التالية:

1. صدور تعديلات أو تشريعات جديدة تؤثر على معالجة البيانات الشخصية أو نقلها.
2. تغيير في طبيعة الخدمات التأمينية أو في أساليب جمع البيانات أو معالجتها.
3. وقوع خرق أمني أو حادث يؤثر على خصوصية بيانات الأفراد.
4. توصيات صادرة عن الجهات الرقابية المختصة مثل وزارة الاقتصاد الرقمي والريادة أو مجلس حماية البيانات.

يُكلف مسؤول حماية البيانات (DPO) بالتنسيق مع الإدارة القانونية والتقنية بإجراء المراجعة وتقديم التوصيات بشأن التحديثات اللازمة مع ضمان توثيق جميع التعديلات وتاريخ دخولها حيز التنفيذ.

كما تلتزم الشركة بإعلام الموظفين والمعنيين بنسخ محدثة من هذه السياسة وتوفيرها من خلال القنوات الرسمية (مثل البريد الإلكتروني الداخلي أو موقع الشركة أو منصة الموظفين).

- 1- نهج العملاء.
- 2- سرية المعلومات المعالجة.
- 3- المعلومات المقدمة من المؤمن عليه.
- 4- المعلومات الواردة في وثيقة التأمين.
- 5- سياسة إدارة المطالبات.
- 6- سياسة إدارة التظلمات.