

سياسة الخصوصية وأمن البيانات

سياسة الخصوصية وأمن البيانات

• المقدمة:

تحدد سياسة الخصوصية وأمن البيانات المبادئ التوجيهية لمؤسسة العاصمة المستقبلية للمقاولات والشركات التابعة لها (المشار إليها فيما بعد باسم المجموعة) لحماية سرية وسلامة وتوافر وخصوصية المعلومات الشخصية القابلة للتحديد (PII) وأمن البيانات. وتلتزم المجموعة بضمان تلبية المتطلبات التشريعية والتنظيمية والتشغيلية والعقدية المتعلقة بالخصوصية وأمن البيانات.

• النطاق:

تطبق السياسة على جميع مجالات العمليات التجارية للمجموعة، وتغطي جميع المديرين والمديرين التنفيذيين والموظفين الذين يعملون لصالح المجموعة أو نيابة عنها. كما تمتد إلى الموظفين المستعان بهم من الخارج أو الموظفين المنتدبين الذين يعملون لصالح المجموعة أو نيابة عنها. تشجع المجموعة الأطراف الخارجية (البائعين/الموردين والمقاولين ومقدمي الخدمات وما إلى ذلك) التي تعمل مع المجموعة على تبني سياسات الخصوصية وأمن البيانات وفقاً لقواعد سلوك الموردين الخاصة بالمجموعة.

• بيان السياسة:

تدرك المجموعة أهمية أخلاقيات البيانات وتحترم حق كل فرد في حماية المعلومات الشخصية. المجموعة هي جامع البيانات ومعالج البيانات للمعلومات التي يتم جمعها ما لم يُنص على خلاف ذلك. تضمن المجموعة الشفافية في ممارسات جمع البيانات وتؤكد على موافقة المستخدم.

• خصوصية البيانات:

- تلتزم المجموعة بإبلاغ الأفراد المعنيين أو مديري المعلومات الشخصية التالية:
- الغرض من جمع المعلومات الشخصية.
- طريقة معالجة المعلومات.
- ضوابط حماية المعلومات الشخصية.
- استخدام أدوات مثل ملفات تعريف الارتباط لجمع المعلومات الشخصية عبر الإنترنت.
- تفاصيل المعلومات مثل عنوان IP ومعلومات المجال التي تم التقاطها عن المستخدم.
- مشاركة المعلومات مع أطراف ثالثة.
- حقوق المستخدم في الوصول إلى المعلومات الشخصية.
- تفاصيل الاتصال بالمجموعة للاستفسارات حول معالجة المعلومات الشخصية.
- التزام المجموعة بالخصوصية والأمان.
- الفترة التي تكون فيها الشروط والأحكام سارية.
- معايير وممارسات أمن المعلومات الخاصة بالمجموعة.
- سياسة الروابط الخارجية.



- نوع المعلومات التي يتم جمعها:

تجمع المجموعة البيانات التي يقدمها الفرد مباشرة للمجموعة عبر وسائل إلكترونية أو مادية بما في ذلك، على سبيل المثال لا الحصر، معلومات التعريف الشخصية والبيانات غير الشخصية، والبيانات التي يتم جمعها بشكل سلبي أو تلقائي مثل المعلومات التي يتم جمعها من متصفح الفرد أو جهازه. تسعى المجموعة إلى الحصول على موافقة صريحة عند الحاجة وتهدف إلى إعلام الأفراد بنوع المعلومات التي يتم جمعها والغرض منها. تهدف المجموعة إلى جمع المعلومات التي تحتاجها فقط لإدارة أعمالها وإنشاء علاقات تجارية والحفاظ عليها والتواصل مع الفرد. ولأغراض أمنية، تمتلك المجموعة كاميرات مراقبة في مبانيها. لا تجمع المجموعة معلومات صريحة عن الأطفال ولا يتم توجيه أي من قنواتها الرسمية إليهم وفقًا للقوانين واللوائح في الولايات القضائية التي تعمل فيها.

- معالجة المعلومات التي يتم جمعها:

لن تستخدم المجموعة معلومات حول أنشطة المستخدم على الإنترنت مع أي معلومات من شأنها أن تؤدي إلى تحديد هوية المستخدم دون موافقته. لن تربط المجموعة المعلومات التي يتم جمعها بواسطة أدوات البرامج (ملفات تعريف الارتباط، صور GIF أحادية البكسل) باسم المستخدم أو عنوان البريد الإلكتروني، في وقت زيارة المستخدم للمواقع. يجوز للمجموعة استخدام معلومات التعريف الخاصة بالمستخدم للتحقيق في الأنشطة غير القانونية المحتملة أو الأنشطة التي تهدد الشبكة أو تنتهك اتفاقية المستخدم الخاصة بهذه الخدمة والمساعدة في منعها.

يجب أن تتم معالجة جميع أنواع البيانات مثل المعلومات الشخصية التي يتشاركها المستخدمون: بشكل عادل وقانوني وآمن.

- معالجة فيما يتعلق بالغرض الذي تم جمعها من أجله.

- أمن البيانات والسرية:

ستنفذ المجموعة إرشادات لحماية خصوصية المعلومات التي يمكن التعرف عليها للمستخدم من الوصول غير المصرح به أو الاستخدام غير السليم وستستمر في تعزيز إجراءات الأمان مع توفر التكنولوجيا الجديدة. تدرس المجموعة تقييم تنفيذ نظام إدارة أمن المعلومات المتوافق مع معايير المنظمة الدولية للمعايير ISO (27001:2022).

تدرس المجموعة التقنيات التالية لحماية المعلومات الشخصية وحماية هوية الأفراد الذين تحتفظ ببياناتهم:

- التشفير القائم على المفتاح.

- إلغاء أو حذف الأحرف داخل مجموعة البيانات.

- تغيير الأرقام والتواريخ.

- استبدال القيم عبر البيانات.

- إخفاء القيمة القائمة على التجزئة.



بالإضافة إلى ذلك، تدرس المجموعة السبل التالية عند وضع استراتيجية لنهجها في التعامل مع الخصوصية وأمن البيانات:

- تنفيذ تقنيات الإخفاء التي تكشف فقط عن الحد الأدنى من البيانات لأي شخص يستخدمها.
- إخفاء أجزاء معينة من البيانات بناءً على طلب الشخص المعني، والسماح فقط لأعضاء معينين من الموظفين بالوصول إلى الأقسام ذات الصلة بهم.
- بناء عملية الخصوصية الخاصة بهم حول إرشادات قانونية وتنظيمية محددة.
- في حالة تنفيذ إخفاء الهوية، يتم الحفاظ على سلامة الخوارزمية المستخدمة لإخفاء البيانات.

- إخفاء البيانات:

تدرس المجموعة تنفيذ تقنيات إخفاء البيانات التالية، مثل إخفاء الهوية وإخفاء الهوية، لحماية هويات الأفراد. علاوة على ذلك، تستخدم المجموعة استراتيجيات مثل الاستبدال العشوائي، والتشفير للحفاظ على التنسيق، والترميز، والإخفاء، والتحرير لضمان أمن البيانات.

- الاحتفاظ بالبيانات والتخلص منها:

يجب الاحتفاظ بجميع أنواع البيانات مثل معلومات التعريف الشخصية التي يتشاركها المستخدمون لمدة لا تزيد عن المدة اللازمة للغرض الذي تم جمعها من أجله. تهدف المجموعة إلى التخلص من البيانات بشكل آمن عند انتهاء فترات الاحتفاظ. مشاركة البيانات ومقدمو الخدمات من جهات خارجية لا تبيع المجموعة أو تُوَجَّر البيانات. عندما تستخدم المجموعة وكلاء أو مقاولين أو شركات أخرى لأداء الخدمات نيابة عنها، ستضمن المجموعة أن الشركة تحمي البيانات التجارية/المالية السرية بما يتفق مع هذه السياسة.

- الحقوق الفردية والموافقة:

تعتقد المجموعة أن الأفراد يجب أن يكون لهم الحق في الوصول إلى بياناتهم أو تصحيحها أو حذفها وفقاً للقوانين واللوائح المعمول بها في الولايات القضائية التي تعمل فيها. تشجع المجموعة الأفراد على الاتصال بالمجموعة على قنواتها الرسمية فيما يتعلق بمخاوفهم بشأن بياناتهم التي يتم جمعها وتخزينها.

ستحترم المجموعة طلبات المستخدمين لمراجعة جميع المعلومات الشخصية التي يتم الاحتفاظ بها في شكل يمكن استرجاعه بشكل معقول، والتي تتكون حالياً من الاسم والعنوان البريدي وعنوان البريد الإلكتروني ورقم الهاتف وستصحح أي معلومات قد تكون غير دقيقة. يمكن للمستخدمين التحقق من إجراء التصحيحات المناسبة. يجب تحديث جميع أنواع البيانات مثل المعلومات الشخصية التي يشاركها المستخدمون والحفاظ عليها دقيقة حسب الضرورة [1] [5]. في حالة تقديم طلبات إلى المجموعة بعدم الاستمرار في استخدام معلوماتهم لتزويد الأفراد بالخدمات، ستحذف المجموعة البيانات المعنية من أنظمة تخزين البيانات الخاصة بها وفقاً لطرق التخلص منها. ومع ذلك، تحتفظ المجموعة بالمعلومات

الضرورية للامتثال للقوانين واللوائح في الولايات القضائية التي تعمل فيها. يجب تزويد المستخدمين بالمعلومات التالية على الأقل قبل جمع المعلومات الشخصية:



- أغراض معالجة المعلومات.

- أي معلومات أخرى تتعلق بالظروف المحددة التي يتم فيها جمع المعلومات الشخصية، مثل:

o مستلمو المعلومات.

o ما إذا كان تقديم المعلومات إلزاميًا أو طوعيًا، وكذلك تأثير عدم تقديم هذه المعلومات.

o وجود الحق في الوصول إلى المعلومات الشخصية أو تحديثها أو إزالتها.

o ما إذا كانت المعلومات الشخصية ستستخدم لأغراض التسويق.

- إخطار انتهاك الخصوصية:

تهدف المجموعة إلى إخطار الأفراد المتضررين والسلطات ذات الصلة حسبما تقتضيه القوانين واللوائح المعمول بها في الولايات القضائية التي تعمل فيها في حالة حدوث انتهاك للخصوصية. تلتزم المجموعة بإعداد مسارات اتصال مناسبة، والتي قد تشمل فرق دعم تكنولوجيا المعلومات وبوابة إلكترونية. تسعى المجموعة بشكل استباقي إلى فرض إجراءات تراقب وتدير انتهاكات الخصوصية وتهدف إلى منع تكرارها. تستخدم المجموعة مجموعة متنوعة من الحلول التكنولوجية الخارجية لتضخيم خدماتها وضمان التجربة المثلى لمستخدميها.

على الرغم من أنها تعطي الأولوية للتعاون مع أطراف خارجية مشهورة وموثوقة، إلا أن المجموعة تؤكد أنها لا يمكن أن تتحمل المسؤولية عن الانتهاكات أو خروقات الأمن على هذه المنصات الخارجية.

ومع ذلك، تتعهد المجموعة بالحفاظ على نهج استباقي لحماية البيانات والتعاون بشكل وثيق مع أطرافها الخارجية لإدارة المضاعفات المحتملة. تنصح المجموعة مستخدميها باليقظة في الدفاع عن معلوماتهم الشخصية، بينما تفكر في كل الجهود المبذولة لحمايتهم. تقترح المجموعة على المستخدمين الالتزام بمعايير السلامة عبر الإنترنت، مثل إنشاء كلمات مرور قوية، وتفعيل المصادقة الثنائية عند الإمكان، وتبني المجموعة على الفور بشأن أي حوادث غير عادية.

- الروابط والمواقع التابعة لجهات خارجية:

قد تحتوي القنوات الرسمية للمجموعة على روابط لمواقع خارجية. المجموعة ليست مسؤولة عن ممارسات الخصوصية لهذه المواقع. تشجع المجموعة الأفراد على توخي الحذر عند مغادرة مواقع المجموعة وقراءة سياسات الخصوصية الخاصة بالمواقع الأخرى. بالإضافة إلى ذلك، تدير المجموعة صفحات وحسابات على مواقع التواصل الاجتماعي للتواصل مع المستخدمين.

المجموعة ليست مسؤولة عن المحتوى على هذه المنصات الذي لم يتم إصداره أو نشره من قبل المجموعة. تحث المجموعة الأفراد على قراءة سياسات الخصوصية لهذه المواقع والتمييز بين المعلومات الصادرة عن المجموعة والمصادر الأخرى. لا تضمن المجموعة المنصات الخارجية التي تستخدمها، ولا المحتوى الذي تنشره جهات خارجية على هذه المنصات.

• إشراك أصحاب المصلحة:

تعزز المجموعة علاقات وثيقة مع أصحاب المصلحة الرئيسيين بحيث يكون هناك فهم واضح لمخاوفهم المتعلقة بالخصوصية. من خلال إشراك أصحاب المصلحة، تحدد المجموعة عوامل الخصوصية المهمة لأصحاب المصلحة وتدمج هذه الاعتبارات في هذه السياسة.



• التدريب والتوعية:

تلتزم المجموعة بالاستثمار المستمر في تدريب وتطوير موظفيها بشأن المسائل المتعلقة بالخصوصية وأمن البيانات. تهدف المجموعة إلى غرس الوعي بشكل منتظم وتعزيز الفهم الواضح للمبادئ الموضحة في هذه السياسة، وتمكين الأفراد من الالتزام بهذه المعايير والتخفيف من المخاطر بشكل فعال.

• الامتثال:

تضمن المجموعة مراقبة منتظمة لأنشطتها للامتثال للقوانين واللوائح المعمول بها في الولايات القضائية التي تعمل فيها. تقوم المجموعة بإجراء عمليات تدقيق داخلية لممارسات الخصوصية وأمن البيانات سنويًا، والإبلاغ عن النتائج لأصحاب المصلحة المعنيين والسعي إلى عمليات تدقيق خارجية لمواءمة التزاماتها مع معايير الصناعة.

• الأدوار والمسؤوليات:

الرئيس التنفيذي مسؤول عن وضع السياسة (بما في ذلك أي تعديلات عليها) ومراقبة امتثالها. مدير تكنولوجيا المعلومات مسؤول عن تنفيذ هذه السياسة والتحسين المستمر أيضًا. جميع الأفراد الذين يعملون لصالح المجموعة أو نيابة عنها مسؤولون عن دعم المبادئ المنصوص عليها في هذه السياسة.

• الإبلاغ والشفافية:

تشجع مؤسسة العاصمة المستقبلية للمقاولات أصحاب المصلحة على الإبلاغ عن المخاوف أو الشكوك أو الانتهاكات المحتملة لهذه السياسة.

• مراجعة السياسة:

تؤمن المجموعة بتحسين أدائها باستمرار من جميع الأنشطة التي تقوم بها أو الخدمات التي تقدمها. ستراجع المجموعة هذه السياسة إذا لزم الأمر، وتراجعها لضمان بقائها محدثة ومتماشية مع مهمة الشركة ورؤيتها وقيمتها الأساسية وقوانينها ولوائحها في البلدان المضيفة لعملياتها، وأفضل الممارسات العالمية. ستتيح المجموعة أي تغييرات على هذه السياسة عبر القنوات المناسبة، وسيكون لكل نسخة تاريخ سريان محدث. يُنصح أصحاب المصلحة بالرجوع إلى القنوات الرسمية للمجموعة للحصول على أحدث سياسة.

تمت مراجعة هذه السياسة آخر مرة في يناير 2025

