الشراكة بين القطاعين العام والخاص في مكافحة الجرائم المالية

حماية البيانات، والتقنية، وتبادل المعلومات مع القطاع الخاص

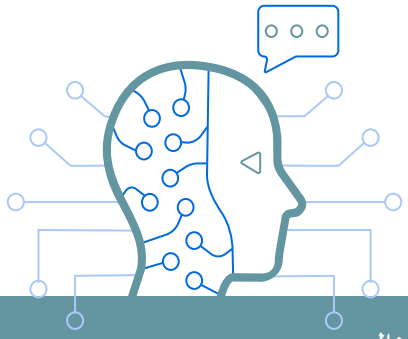
أبرز التوصيات من أجل تحقيق التعاون المسؤول بفاعلية

يساعد التعاون وتبادل المعلومات المؤسسات المالية على بناء صورة أوضح للمعاملات المشبوهة والشبكات الإجرامية، وفهم مخاطر غسل الأموال وتمويل الإرهاب وانتشار التسلح وتقييمها وتخفيفها بشكل أفضل. ويمكنه أيضاً تزويد السلطات المختصة بمعلومات استخباراتية ذات جودة أعلى تساعد في رفع قدراتها على التحقيق في هذه الجرائم ومقاضاة مرتكبيها، والمساهمة في نهاية المطاف في الحد من حدوث الجرائم ومنع وصول آثارها إلى المجتمع.

ومع ذلك، لابد أن يتم تصميم مبادرات التعاون هذه وتنفيذها بفاعلية وبشكل مسؤول، ووفقاً لأنظمة حماية البيانات والخصوصية، بحيث تتم مراعاة المخاطر المترتبة على المشاركة المتزايدة للبيانات الشخصية بشكل مناسب.

اعتمدت مجموعة العمل المالي (فاتف) في صياغة هذه التوصيات للقطاعين العام والخاص على الدروس المستفادة من تجارب الدول الأعضاء لتجنب المخاطر الشائعة. وتنطوي مبادرات التعاون الناجحة مع القطاع الخاص على عدة عوامل أولها تضمين مجموعة من أصحاب المصلحة، والأخذ في الاعتبار النظام والسياق المحلي للمنطقة، واتباع نهج مرحلي وتعزيز ثقة وفهم العامة. بالطبع لا يوجد حل واحد يناسب جميع المؤسسات المالية حول العالم ويعالج كافة أهداف حماية البيانات والخصوصية في مجال مكافحة غسل الأموال وتمويل الإرهاب وتمويل انتشار التسلح. لذا ينبغي النظر في كل مبادرة لمشاركة البيانات على أساس كل حالة على حدة بالاعتماد على خصائصها الفريدة ومتطلبات الخصوصية وحماية البيانات ذات الصلة.

قد تساعد التوصيات التالية الدول أو كيانات القطاع الخاص الساعية لتعزيز تبادل المعلومات. كما يجدر الذكر أن هذه التوصيات تستند إلى الملاحظات والدروس المستفادة من تجارب الدول الأعضاء.



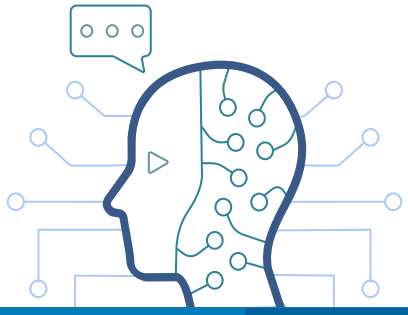
التوصيات الخاصة بالقطاع العام

ينبغي على القطاع العام اتخاذ دورأكثر فعالية في تسهيل الشراكة، على سبيل المثال:

- تحديث الأطر القانونية أو الرقابية إذا لزم الأمر لتوفير أساس قانوني واضح لمشاركة ومعالجة البيانات بما يتماشى مع الاعتبارات المتعلقة بحماية البيانات والخصوصية.
- تسليط الضوء على الجرائم أو الأنماط المحددة أو أنواع البيانات الرئيسية التي سيستفاد أكثر من مشاركتها، من أجل مواءمة مبادرات مشاركة البيانات مع الأهداف الوطنية لمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح.
- تحديد كيان قيادي أو جهة اتصال معينة مسؤولة عن مبادرة تبادل معلومات القطاع الخاص للحفاظ على استمرارية الحوار مع الجهات المعنية بحماية البيانات والجهات الحكومية الأخرى وضمان اتساق المشورة.
- توفير أدلة إرشادية أو قوائم مرجعية حول الضوابط ذات الصلة بشكل مستمر لمساعدة القطاع الخاص على الفهم والتعامل مع متطلبات مكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح، وحماية البيانات، والمتطلبات الأخرى ذات الصلة.
- الاستفادة من بيئات الاختبار التنظيمية (regulatory sandboxes) والبرامج التجريبية لاختبار مبادرات مشاركة البيانات، وفهم الآثار المترتبة على السياسات، وبناء الثقة، ويُفضّل أن يتم ذلك بمشاركة كل من الجهات المعنية بحماية البيانات والسلطات المختصة بمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح.
- بناء منصة آمنة لتبادل المعلومات مع القطاع الخاص لتوفير الموارد المالية والتقنية المطلوبة وضمان إمكانية الوصول والقدرة على تحمل التكاليف للمؤسسات.
- تطوير مشاريع لمواءمة البيانات وتوحيدها، على سبيل المثال: تحديد معايير وتعريفات البيانات المشتركة أو إطلاق مبادرات هيكلة وتنقية البيانات.

ضمان وتعزيز الحوار المنتظم بين الجهات المعنية بحماية البيانات والسلطات المختصة بمكافحة غسل الأموال وتمويل الإرهاب و انتشار التسلح (بما في ذلك على المستوى الدولي)، على سبيل المثال:

- عقد محافل ومنتديات بانتظام بين السلطات المختصة بمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح والجهات المعنية بحماية البيانات ومؤسسات القطاع الخاص لتبادل الخبرات ومناقشة التحديات وتطوير العلاقات.
- وضع استراتيجية مشتركة لتبادل المعلومات مع ضمان تدابير مناسبة لحماية البيانات والخصوصية لتشجيع المبادرات في القطاع.
- توفير إرشادات مشتركة أو إتاحة مشاركة الجهات على مستوى القطاع فيما يتعلق بمتطلبات حماية البيانات والخصوصية والحلول التقنية.
- دعم السلطات المختصة بمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح للمبادرات في القطاع والمساهمة في بناء جسور الشراكة بين القطاع الخاص والجهات المعنية بحماية البيانات.



التوصيات الخاصة بالقطاع الخاص

ينبغي على القطاع الخاص الاستفادة من تقنيات تعزيز الخصوصية

- بالرغم من أن تقنيات تعزيز الخصوصية ليست "حلاً سحرياً"، إلا أنها يمكن أن تساعد في دعم الالتزام بأنظمة حماية البيانات والخصوصية.
- عند القيام بذلك، تنبغي مراعاة قابلية التشغيل المشترك بين الأنظمة وإمكانية الوصول إلى التقنيات المختلفة لتعزيز المشاركة في القطاع على نطاق أوسع.
- تناول تقرير التقييم للمرحلة الأولى (Phase 1 Stocktake Report) بالتفصيل التقنيات المختلفة التي من الممكن تطبيقها والمخاطر والفرص التي قد تشكلها.

ضمان تناسق البيانات

- تعمل التقنيات المخصصة لمشاركة البيانات، وخاصةً التحليلات المتقدمة، بشكل أفضل مع المعايير والصيغ الموحدة للبيانات مما يؤدي أيضاً إلى تحسين دقة البيانات وموثوقيتها.
- في مرحلة تصميم المبادرات، يمكن للمؤسسات الاستفادة من البيانات الموجودة والمعدة بتنسيق منظم، على سبيل المثال. مجالات البيانات المستخدمة في نظام سويفت (SWIFT) أو تنفيذ مبادرات تنقية/هيكلة البيانات (بما في ذلك عن طريق إشراك مقدمي خدمات التقنية).

السعي لتطبيق مبدأ حماية البيانات خلال مرحلة التصميم

- تجب مراعاة مبادئ حماية البيانات والخصوصية في مرحلة التصميم (المرحلة الأولية) لمبادرة تبادل المعلومات. حيث يساعد تقييم تأثير حماية البيانات (Data Protection Impact Assessment) على تقييم درجة الالتزام وتحديد المخاطر وتخفيفها. كما يسمح للمشاركين بإدارة المشاريع لتتماشى مع متطلبات حماية البيانات والخصوصية ذات الصلة، وبالتالي توفير الموارد.
- إن اتفاقيات/عقود مشاركة البيانات تحدد بوضوح المسؤوليات وتضع إطاراً للتعامل مع أي شكاوى من العملاء.
- يساعد تقييم الأثر على حقوق الإنسان (Human Rights Impact Assessment) في ضمان الامتثال لالتزامات حقوق الإنسان (مثل الحق في الخصوصية).
- يساعد تقييم المصلحة المشروعة (Legitimate Interest Assessment) مراقبي البيانات على تحديد المصلحة المشروعة لمشاركة البيانات، وتقييم ما إذا كانت المعالجة ضرورية لتحقيق هذه المصلحة، وموازنة المصلحة مع المصالح والحقوق والحريات الفردية.

تأسيس تعاون مبكرومستمر مع الجهات المعنية بحماية البيانات

- يعتبر تضمين الجهات المعنية بحماية البيانات أمراً بالغ الأهمية لنجاح أي مشروع لتبادل المعلومات، ويجب أن يبدأ التعاون مبكراً في مرحلة التصميم، ويستمر حتى إعداد تقييم تأثير حماية البيانات وأن يكون على أساس منتظم في حين يتم البدء بجمع وتحليل البيانات.
- كما يعتبر تضمين السلطات المختصة بمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح أمراً هاماً أيضاً في نجاح المبادرات التي يقودها القطاع الخاص.

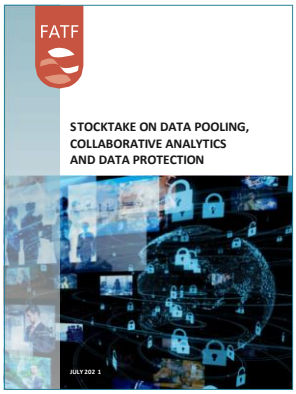
وضع مؤشرات لقياس النجاح

- إن وضع مؤشرات أداء واضحة يُمكّن المشاركين من تقييم ما إذا كانت المبادرة تحقق غرضها وتحدد ما إذا كان تبادل المعلومات لا يزال ضرورياً / مقبولاً / متناسباً بما يتماشى مع متطلبات الخصوصية وحماية البيانات المعمول بها.
- تساعد مشاركة المخرجات والنتائج الإيجابية على بناء الثقة وتشجيع المشاركة على نطاق أوسع.

يمكن الحصول على النسخة الكاملة من التقارير من خلال:

الشراكة بين القطاعين العام والخاص في مكافحة الجرائم المالية: حماية البيانات، والتقنية، وتبادل المعلومات مع القطاع الخاص

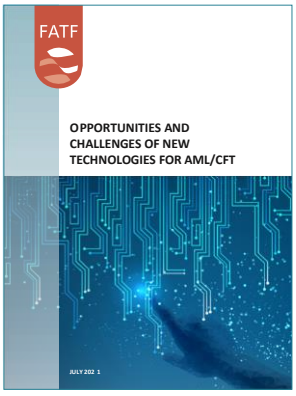
يوليو ٢٠٢٢



حصر وجرد أنظمة جمع البيانات والتحليلات التعاونية وحماية البيانات

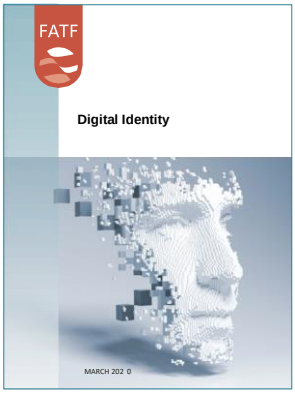
يوليو ٢٠٢١

ومتاحة أيضا التقارير التالية ذات الصلة على موقع الفاتف www.fatf-gafi.org:



فرص وتحديات التقنيات الجديدة لمكافحة غسل الأموال وتمويل الإرهاب

يونيو ٢٠٢١



الدليل الإرشادي للهوية الرقمية الصادر من مجموعة العمل المالي (فاتف)

فبراير ٢٠٢٠

تمت ترجمة هذا التقرير الصادر عن مجموعة العمال المالي إلى اللغة العربية من قبل اللجنة الدائمة لمكافحة غسل الأموال في المملكة العربية السعودية بتصريح من مجموعة العمل المالي ويعد التقرير المنشور باللغة الإنجليزية على موقع المجموعة هو النسخة المعتمدة في حال وجود تعارض أو اختلاف بالترجمة.

Copyright © FATF/OECD. All rights reserved.