الرقم: ١٨٩٤٢ /٦/١٠

التاريخ: ٤ / ٥ / ١٤٤٤

الموافق: ٢٨ /١١/ ٢٠٢٢

تعليمات تنظيم إجراءات عمل الخدمات المالية المفتوحة

رقم (١٣/٢٠٢٢)

صادرة استناداً لأحكام المادة (٦٥/ب) من قانون البنك المركزي الأردني رقم (٢٣) لسنة ١٩٧١ وتعديلاته والمادة (٩٩/ ب) من قانون البنوك رقم (٢٨) لسنة ٢٠٠٠ وتعديلاته واستناداً لأحكام المادة (٥٥) من نظام الدفع والتحويل الإلكتروني للأموال رقم (١١١) لسنة ٢٠١٧.

المادة (١):

أ. تسمى هذه التعليمات "تعليمات تنظيم إجراءات عمل الخدمات المالية المفتوحة"، ويعمل بها من تاريخ إصدارها.

ب. على كل شركة تقوم بتقديم خدمات مالية مفتوحة توفيق أوضاعها حسب أحكام هذه التعليمات خلال سنة من تاريخ نفاذها وللبنك المركزي أن يمدد هذه المدة.

المادة (٢):

أ. يكون للكلمات والعبارات التالية حيثما وردت في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة أو السياق على خلاف ذلك:

الكلمة/العبارة	المعنى
الشركة	أي بنك مرخص له ممارسة الأعمال المصرفية في المملكة حسب أحكام قانون البنوك وأي شركة دفع وتحويل الكتروني للأموال مرخص لها بالعمل في المملكة حسب أحكام نظام الدفع والتحويل الإلكتروني للأموال رقم (١١١) لسنة ٢٠١٧.
المجلس	مجلس إدارة الشركة ومن في حكمه.

الإدارة التنفيذية العليا	تشـمل مدير عام الشـركة أو المدير الإقليمي ونائب المدير العام أو نائب المدير الإقليمي ومسـاعد المدير العام أو مسـاعد المدير الإقليمي والمدير المالي ومدير التدقيق الداخلي ومدير إدارة المخاطر ومدير الامتثال، بالإضافة لأي موظف في الشركة له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين ويرتبط وظيفياً مباشرةً بالمدير العام.
واجهة برمجة التطبيقات (APIs) Application Programming Interfaces	هي مجموعة من القواعد والمواصـفات والبروتوكولات والأدوات اللازمة لإنشاء واجهة وسيطة بين برامج التطبيقات المختلفة وتسمح لها بالتواصل وتسهيل عملية التفاعل فيما بينها.
حساب العميل	حسـاب مالي للعميل لدى الشـركة يحتوي على بيانات العميل وفق طبيعة عمل الشركة.
بيانات العميل	أي معلومات أو بيانات عن العملاء أو حسـاباتهم الخاصـة بهم أو أي من معاملاتهم الموجودة لدى الشركة.
الخدمات المالية المفتوحة (Open Finance)	الخدمات التي تهدف إلى تمكين عملاء الشركة من مشاركة بياناتهم المالية بشـكل آمن مع مزودي الطرف الثالث (TPP) لفتح المجال لتقديم خدمات ومنتجات مالية ذات قيمة مضـافة للعملاء من خلال تقنية واجهة برمجة التطبيقات API .
مزود خدمة معلومات الحساب (AISP) Account Information Service Provider	هي الجهة التي تمتلك المقدرة الفنية والمخول لها من قبل العميل (بموجب موافقة العميل الصـريحة) الوصـول إلى بيانات/معلومات حسـابه لدى الشـركة واسـتخدامها لبناء وتقديم خدمات ذات قيمة مضـافة عن طريق معالجة البيانات ويقوم بتوفير نقطة وصـول بديلة إلى مصـادر متعددة للبيانات بخلاف تلك النقاط المملوكة من قبل الشركة.
مزود خدمة البدء في الدفع (PISP) Payment Initiation Service Provider	الجهة التي تمتلك المقدرة والمخول لها من قبل العميل (بموجب موافقة العميل الصـريحة) إما بتمكينه من تمرير طلب حركة دفع فقط و/أو إجراء عملية الدفع من خلاله بالنيابة عن العميل.
مزود الطرف الثالث (TPP) Third Party Provider	الجهة التي تستخدم واجهة برمجة التطبيقات (API) للوصـول إلى بيانات العميل من أجل تقديم خدمات ومنتجات مالية ذات قيمة مضافة للعملاء من خلال تقنية واجهة برمجة التطبيقات API. ومنهم على سـبيل المثال لا الحصـر مزودي خدمة البدء في الدفع (PISPs) و / أو مزودي خدمة معلومات الحساب (AISPs).
المشارك	هو الطرف المشـمول بمنظومة الخدمات المالية المفتوحة وهم الشـركة و مزود الطرف الثالث (TPPs)

موافقة العميل الصريحة	موافقة مسبقة خطية أو ما يعادلها وفق التشريعات ذات العلاقة من العميل صاحب الحساب تخول الشركة بمشاركة بياناته.

ب. تعتمد التعاريف الواردة في قانون البنك المركزي وقانون المعاملات الإلكترونية وقانون البنوك ونظام الدفع والتحويل الإلكتروني للأموال وأية تشريعات ذات علاقة صادرة عن البنك المركزي حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

ج. تعتبر الأحكام الواردة في تعليمات تنظيم إجراءات اعرف عميلك والتعامل معه الكترونيا (٢٠٢١/٧) متطلبات إضافية لما جاء في هذه التعليمات وتقرأ معها كوحدة واحدة.

د. تعتبر الأحكام الواردة في هذه التعليمات متطلبات إضافية لما جاء في تعليمات مكافحة غسل الأموال وتمويل الإرهاب وتقرأ معها كوحدة واحدة.

المادة (٣): نطاق وآلية التطبيق والأطراف المعنية

أ. مع مراعاة ما ورد في الفقرة (ب) من هذه المادة تسري أحكام هذه التعليمات على جميع البنوك العاملة في المملكة وشركات الدفع والتحويل الإلكتروني للأموال المرخصة في المملكة.

ب. على فروع البنوك/شركات الدفع والتحويل الإلكتروني للأموال الأجنبية العاملة في المملكة الالتزام بهذه التعليمات بالقدر الذي ينطبق عليها أو بدليل وسياسات الصادرة عن البنك/الشركة الأم أو السلطة الرقابية في الدولة الأم أيهما أكثر تحقيقاً لأهداف هذه التعليمات، وفي حال كانت التعليمات الصادرة عن البنك/الشركة الأم أو السلطة الرقابية في الدولة الأم أكثر تحقيقاً لأهداف التعليمات على الفرع، فإن على هذا الفرع تقديم ما يؤيد ذلك إلى البنك المركزي، مع مراعاة عدم التعارض مع التشريعات النافذة في المملكة، وفي حال وجود تعارض فعلى الفرع إعلام البنك المركزي والبنك/الشركة الأم بذلك وتقديم التوضيح اللازم لهذا التعارض والحصول على موافقة البنك المركزي على أسلوب معالجة هذا التعارض.

المادة (٤): الحاكمية

أ. يتولى المجلس المسؤوليات والمهام التالية:

1. ضمان وجود أنظمة ضبط ورقابة داخلية مناسبة وفعالة ومتابعتها من خلال مراعاة فهم المخاطر الرئيسية المتعلقة بالخدمات المالية المفتوحة التي تواجه الشركة مع ضمان اتخاذ الإجراءات اللازمة لتحديد ومراقبة هذه المخاطر.
2. اعتماد سياسة الخدمات المالية المفتوحة وتعديلاتها.

ب. تتولى الإدارة التنفيذية العليا المسؤوليات والمهام التالية كل بحسب موقعه:

1. الإشراف على وضع وتنفيذ سياسة الخدمات المالية المفتوحة ومراجعتها وضمان تحديثها بشكل دوري.
2. ضمان الحصول على رأي إدارة الامتثال في الشركة قبل التعاقد مع مزود الطرف الثالث (TPP)
3. ضمان تضمين خطط استمرارية العمل والتعافي من الكوارث لدى الشركة سيناريوهات التعطل والاختراق المحتملة والخاصة بالتعامل مع مزود الطرف الثالث (TPP) واختبارها بشكل دوري.

4. ضـــمان تنظيم العلاقة مع مزود الطرف الثالث (TPP) بموجب اتفاقيات تعاقدية مكتوبة بشـــكل واضـــح وصريح، تحدد أدوار ومهام ومسؤوليات وحقوق كلا الطرفين وسرية وخصوصية وأمن المعلومات وعدم الإفصاح عنها، وتحديد أحكام إنهاء التعاقد فيما بينهم.
5. ضـــمان الحصـــول على موافقة العميل الصـــريحة وذلك بما يتوافق مع القوانين والتعليمات النافذة ذات العلاقة بالخدمات المالية المفتوحة وبما يشمل:
   أ. لدى إتاحة وصول مزود الطرف الثالث (TPP) لحسابه أو لأي من بياناته.
   ب. للخدمات التي تتطلب طبيعتها تخزين بيانات للعميل لدى مزود الطرف الثالث (TPP).
6. ضـــمان مراجعة جميع الأنشـــطة والخدمات التي يحق لمزود الطرف الثالث (TPP) القيام بها أو تقديمها، وإخطار المجلس بانتظام عن المخاطر التي قد تنشأ عنها.
7. ضـــمان تدريب وتثقيف وتوعية موظفيها حول الأعمال ذات العلاقة التي ســـيقدمها مزود الطرف الثالث (TPP)، وكيفية ارتباطها بأعمالهم.
8. إبلاغ البنك المركزي فورا بأي مخالفة أو انتهاك للقوانين والأنظمة والتعليمات النافذة أو أي تطورات سلبية خلال إجراءات التعاقد مع مزود الطرف الثالث (TPP) والتي من شأنها أن تؤثر سلبا على الشركة وإجراءات الشركة.

المادة (٥): سياسة الخدمات المالية المفتوحة

أ. تلتزم الشـركة بوضـع سـياسـة للخدمات المالية المفتوحة بحيث تكون موثقة ومعتمدة، وتغطي كافة العناصـر الأمنية المتعلقة بها، وأن تكون مبنية على أفضـل الممارسـات العالمية بالخصـوص ومتوافقة مع سـياسـة أمن المعلومات والأمن السيبراني لدى الشركة، ويجب أن تتضمن السياسة بحد أدنى ما يلي:

1. وضع إجراءات عمل تفصيلية وواضحة لتنظيم التعامل مع مزود الطرف الثالث (TPP).
2. البيانات والمعلومات والعمليات والخدمات المراد إتاحة الوصول لها من خلال مزود الطرف الثالث (TPP).
3. أسس التعاقد مع مزود الطرف الثالث (TPP) والحد الأدنى من المتطلبات الواجب توفرها لدى مزود الطرف الثالث (TPP) قبل الدخول في أي علاقة تعاقدية معه.
4. أسس تقييم مزود الطرف الثالث (TPP) حول قدرته على استخدام حلول تقنية قادرة على التفاعل مع البرامج والأنظمة التي تستخدمها الشركة دون أي تعديلات جوهرية على أنظمته.
5. المعايير الفنية والتقنية والضوابط الأمنية الواجب اتباعها عند التعامل مع أي مزود الطرف الثالث (TPP).
6. آلية مناسبة للمراقبة المستمرة والتدقيق على مزود الطرف الثالث (TPP) وفقا لشروط وأحكام الاتفاقية الموقعة بين الشركة ومزود الطرف الثالث (TPP).
7. أدوار ومسؤوليات المعنيين لدى الشركة بخصوص التعامل مع مزود الطرف الثالث (TPP).
8. أسس تقييم مخاطر التعامل مع مزود الطرف الثالث (TPP) وآليات وضوابط إدارتها والتخفيف منها.

ب. تلتزم الشركة بنشر أهم بنود سياسة الخدمات المالية المفتوحة والتي لا تعتبر بنود سرية على القنوات الرسمية والمعتمدة لديها.

المادة (٦): إدارة المخاطر

على الشـــركة تحديد وإدارة ومراقبة أية مخاطر قد تنتج عن التعاقد مع مزود الطرف الثالث (TPP) وتضمينها ضمن إطار تقييم المخاطر الشامل للمؤسسة المالية وتحديثه، مع الأخذ بعين الاعتبار ما يلي:

أ. تحديد درجة حســاســية أصــول المعلومات والبيانات التي يتم الوصــول إليها من قبل مزود الطرف الثالث (TPP).

ب. تحليل وتقييم أثر التعامل مع مزود الطرف الثالث (TPP) على ملف مخاطر الشـركة وتحقيق أهدافها، والقيام بتوثيقهما وتضمينها ضمن سجل المخاطر الخاص بالشركة.

ج. تقييم المخاطر الأمنية والتشــغيلية الشــاملة المرتبطة بالتعامل مع مزود الطرف الثالث (TPP) وتحديد دور ومسؤولية الشركة في إدارتها وتوثيق هذا التقييم ومستوى المخاطر المقبول.

د. وضع خطة لتخفيف من المخاطر الأمنية والتشغيلية التي قد تنتج عن التعاقد مع مزود الطرف الثالث (TPP).

ه. وضــع معايير مخاطر رئيســية (Key Risk Indicators) لمراقبة مســتوى المخاطر المتعلقة بالتعامل مع مزود الطرف الثالث (TPP) للتأكد من عدم تجاوز المخاطر المقبولة (Risk Appetite) ودرجة تحمل المخاطر.

و. وضــع منهجية لتصــنيف عمليات الدفع بناءً على المخاطر التي من الممكن أن تتعرض لها تلك العمليات وتناسبها مع عدد فئات التوثق المستخدمة لتحديد هوية العميل عند إجراء عمليات الدفع.

المادة (٧): التعاقد مع مزود الطرف الثالث (TPP)

أ. على الشــركة عند التعاقد مع مزود الطرف الثالث (TPP) مراعاة ما يلي وذلك بالحد الأدنى وبحدود العقد المبرم بينهم:

1. وجود علاقة تعاقدية مكتوبة وواضــحة بين العميل ومزود الطرف الثالث (TPP) تحدد أدوار ومهام ومسؤوليات وحقوق كلا الطرفين.
2. وجود سياسة امن وحماية المعلومات وخطط استمرارية العمل والاستجابة لحوادث الأمن السيبراني لدى مزود الطرف الثالث (TPP) والتأكد من فعاليتها.
3. قيام مزود الطرف الثالث (TPP) بتعيين جهة خارجية مســتقلة متخصــصــة لإجراء تقييم نقاط الضــعف والثغرات الأمنية مرة واحدة على الأقل كل ٦ أشــهر، واختبار الاختراق مرة واحدة ســنويا على الأقل أو بعد أي تغيير جذري لديه.
4. ضمان المقدرة على التدقيق والمراقبة على مزود الطرف الثالث (TPP).
5. ضــمان القدرة على تحديد الحد الأدنى والأعلى للعمولات التي يتقاضــاها مزود الطرف الثالث (TPP) وفق الأوامر الصادرة عن البنك المركزي.
6. للبنك المركزي الحق بالتفتيش على مزود الطرف الثالث (TPP) وبحدود الخدمات المالية المفتوحة التي يقدمها من الموظفين المفوضين من البنك المركزي أو أي طرف خارجي يعينه البنك المركزي وعلى نفقة الشــركة، وتلتزم الشــركة ومزود الطرف الثالث (TPP) بالتعاون معهم بما يمكنهم من القيام بأعمالهم بشكل كامل.

ب. تلتزم الشـــركة بإعلام البنك المركزي خلال (١٥) يوم كحد أقصـــى من تاريخ التعاقد مع مزود طرف ثالث (TPP) وبعد إنهاء التعاقد معه.

المادة (٨): متطلبات واجهة برمجة التطبيقات

على الشركة السماح لمزود الطرف الثالث (TPP) الوصول إلى البيانات وحسابات العملاء وذلك باستخدام واجهة برمجة التطبيقات (API)، لتمكينه من تقديم الخدمات المالية المفتوحة للعملاء وبحيث تضمن الشركة توفر ما يلي بالحد الأدنى:

أ. توفير وتطوير واستمرارية وتهيئة واجهة برمجة تطبيقات واحدة على الأقل لمزودي الطرف الثالث (TPP) سواء كانت مخصصة فقط لمزودي الطرف الثالث (TPP) أو الواجهة المستخدمة لعملاء الشركة.

ب. التأكد من هوية مزود الطرف الثالث (TPP) الذي يحاول الوصـول إلى البيانات والحسـابات المتاحة من قبل الشركة.

ج. المقدرة على حجب البيانات والحسـابات عن الجهات غير المخولة بالوصـول اليها وتوفير ضـوابط الحماية اللازمة ضد أي محاولات لهجمات سيبرانية أو التلاعب بها.

د. الحفاظ على سرية وأمن البيانات الخاصة بالشركة والعملاء

ه. استخدام آليات تشفير مناسبة ومحكمة عند تبادل البيانات والمعلومات عبر واجهة برمجة التطبيقات (API) مع مزود الطرف الثالث (TPP).

و. تناسب واجهة برمجة التطبيقات مع طبيعة المهام التي سيقوم بها مزود الطرف الثالث (TPP).

ز. تسـجيل وصـول مزود الطرف الثالث (TPP) إلى حسـابات العملاء في سـجلات الوصـول التابعة للشـركة وسجلات الوصول التابعة لمزود الطرف الثالث (TPP) والعمليات التي تتم عليها وإمكانية الرجوع اليها عند الحاجة وتحديد مدد الاحتفاظ بها وفق التشريعات النافذة بالخصوص.

ح. ضمان أمان جلسات الاتصال (Communication Sessions) بين المشاركين والعميل.

ط. ضمان الاحتفاظ بسجلات جلسات الاتصال بين المشاركين والعميل حسب التشريعات ذات العلاقة.

ي. ضمان قصر مدة جلسات الاتصال قدر الإمكان وإنهاء الجلسات فور استكمال العمل المطلوب.

ك. ضمان قدرة الشركة على منع/إيقاف مزود الطرف الثالث (TPP) من الوصول غير المصرح به إلى البيانات أو تخزينها أو معالجتها لأغراض أخرى غير تقديم الخدمات المسموح بتقديمها والمتفق عليها.

ل. وجود ضوابط لإدارة وصول العملاء للخدمات المقدمة من مزود الطرف الثالث (TPP) .

م. على الشـركة تحديد مؤشـرات الأداء الرئيسـية والأهداف التشـغيلية للخدمة لقياس توافر وأداء واجهة برمجة التطبيقات الموفرة لمزود الطرف الثالث (TPP)على أن تتسـم بالشـفافية وان تكون على الأقل بنفس مسـتوى المؤشرات والتوافر والأداء والأهداف الخاصة بالواجهة المخصصة للشركة المتاحة أمام عملاء الشركة.

ن. ضمان عدم تأثير الخدمات المقدمة من قبل مزود الطرف الثالث (TPP) على خدمات وسمعة الشركة.

س. ضمان عدم تأثير تعطل أو عدم كفاءة أداء الواجهة المخصصة لمزودي الطرف الثالث (TPP) على تقديم الخدمات من قبل الشركة.

ع. ضمان أن تكون جميع المواصفات الفنية لأي من الواجهات موثقة بحيث تحدد مجموعة من الإجراءات والبروتوكولات والأدوات اللازمة لمزودي الطرف الثالث بهدف السماح لبرامجهم وتطبيقاتهم من التعامل مع الأنظمة الخاصة بالشركة.

ف. إعلام والتنسيق مع مزود الطرف الثالث (TPP) عن أي تغيير على المواصفات الفنية الخاصة بواجهة برمجة التطبيقات بحيث يضمن عدم انقطاع الخدمات المقدمة من قبله.

ص. توفير منصة تجريبية لتمكين مزودي الطرف الثالث (TPP) من تجربة برامجهم وتطبيقاتهم المستخدمة لتوفير الخدمات المالية المفتوحة، بحيث لا يتم مشاركة أي معلومات سرية من خلال هذه المنصة.

ق. ضمان عدم إمكانية قراءة بيانات العملاء من قبل أي من موظفين غير المصرح لهم من المشاركين.

ر. على الشركة عند تصميم واجهة برمجة التطبيقات تضمين استراتيجيات وخطط لمواجهة الطوارئ في حال حدوث توقف في عمل الواجهة أو تعطل في أنظمتها مع مراعاة ما يلي:

1. أن تتضمن خطط مواجهة الطوارئ خطط الاتصال لإبلاغ مزودي الطرف الثالث (TPP) بالتدابير اللازمة لاستعادة الخدمة حسب الخيارات البديلة الممكنة والمتوفرة وبشكل فوري.
2. الاتفاق مع مزودي الطرف الثالث (TPP) على آلية رفع تقارير بالمشاكل المتعلقة بواجهة برمجة التطبيقات.
3. إخطار المشاركين في منظومة الخدمات المالية المفتوحة بذلك.

ش. على الشركة مراعاة ما يلي عند تبادل البيانات و/أو المعلومات مع مزود الطرف الثالث (TPP):

1. تزويد مزود خدمة معلومات الحساب (AISP) بنفس بيانات و/أو المعلومات من حساب العميل المحدد وحركات الدفع المرتبطة به والمتاحة للعميل مستخدم الخدمات المالية المفتوحة عند طلبها بشكل مباشر.
2. تزويد مزودي خدمة البدء بالدفع (PISP) بنفس البيانات و/أو المعلومات حول بدء وتنفيذ حركة الدفع التي يتم توفيرها للعميل مستخدم الخدمات المالية المفتوحة عند بدء الحركة بشكل مباشر من الشركة.
3. تزويد مزودي خدمة البدء بالدفع (PISP) فيما إذا كان المبلغ اللازم لتنفيذ حركة الدفع متوفرا في حساب الدافع.
4. في حال وقوع خطأ أو حدث غير متوقع أثناء تبادل البيانات على الشركة إرسال إشعار إلى مزود الطرف الثالث (TPP) لتفسير سبب الحدث أو الخطأ الغير متوقع.
5. تصميم واجهة برمجة التطبيقات بحيث يقتصر وصول مزود الطرف الثالث (TPP) فقط إلى البيانات التي يمتلك الإذن بالاطلاع عليها أو معالجتها وأن يتم توثيق حقوق الوصول هذه بشكل مناسب والتحقق منها ومراجعة حقوق الوصول هذه بشكل دوري (مرتين سنويا على الأقل).

المادة (٩): معايير ومتطلبات مزود الطرف الثالث (TPP)

على الشركة اتخاذ إجراءات العناية الواجبة الكافية للتعرف على هوية مزود الطرف الثالث (TPP) وبما يتوافق مع المخاطر التي قد تنتج عن التعاقد معه والتحقق منها بالطرق المناسبة ووفق سياسة الخدمات المالية المفتوحة والأنظمة والتعليمات والتشريعات المعمول بها، والمتابعة المتواصلة بموجب العلاقة التعاقدية المبرمة معه، وأن يتم الأخذ بعين الاعتبار الحد الأدنى من المتطلبات أدناه لدى التعامل مع كل من:

أ. مزود خدمة معلومات الحساب (AISP)

1. أن يكون شركة محلية أو فرع شركة أجنبية مرخصة ومسجلة من قبل الجهات الرقابية المعنية في الأردن، لديها السمعة الجيدة والخبرة والكفاءة التقنية والفنية والقدرة على تلبية متطلبات الشركة وعميلها.
2. أن يكون قادرًا على إجراء الاتصال الآمن لطلب واستقبال البيانات و/أو المعلومات على واحد أو أكثر من حسابات العميل المحددة والحركات المالية المرتبطة بها.
3. أن يكون قادرًا على توفير آليات مناسبة وفعالة لمنع الوصول إلى المعلومات إلا من خلال حسابات العميل المحددة والحركات المالية المرتبطة بها وبناءً على موافقة العميل الصريحة.
4. ضمان عدم الخطأ في إرسال وتوجيه البيانات و/أو المعلومات في حال وجود أكثر من جلسة اتصال واحدة.
5. وضع آلية لمعالجة شكاوى العملاء فيما يخص الخدمات التي يوفرها مزود الطرف الثالث (TPP)، وتحديد المهام والمسؤوليات بناء على سيناريوهات مختلفة وإتاحتها للعملاء.
6. ضمان وجود ضوابط داخلية أمنية ورقابية مطبقة لدى مزود الطرف الثالث (TPP) وملاءمتها مع طبيعة وحساسية البيانات المتاح الوصول إليها.
7. تقديم خطة عمل تفصيلية للشركة وذلك للخدمات التي سيقوم بها وفق العقد المبرم فيما بينهما.
8. ضمان قيام المدقق الخارجي للمزود الطرف الثالث (TPP) إبلاغ الشركة عن مواطن الضعف في أنظمة الضبط والرقابة الداخلية أو التراجع في الأداء المالي لدى مزود الطرف الثالث (TPP).
9. الامتثال للتشريعات ذات العلاقة المعمول بها بالمملكة.
10. امتلاك سياسات وإجراءات للكشف عن الاحتيال ومنعه.
11. القدرة على حفظ البيانات بطرق آمنة تحد من محاولات الهجوم السيبراني.
12. حماية جلسات الاتصال (Communication Sessions) من الوصول إلى البيانات المرسلة ومن التلاعب بها من قبل الأطراف غير المصرح بهم.

13. عدم طلب أي بيانات و/أو معلومات إضافية لا تتطلبها الخدمة المقدمة من قبله للعملاء.

14. حماية البيانات و/أو المعلومات التي يمتلك حق الوصول اليها من قبل الشركة وضمان عدم الوصول أو الاطلاع من قبل أطراف أخرى غير مصرح لها.

15. عدم استخدام البيانات أو تخزينها أو معالجتها لأغراض أخرى غير تقديم الخدمات المسموح له بتقديمها.

16. عدم تخزين أية بيانات حساسة تخص العملاء بموجب تصنيف الشركة المعتمد للبيانات والمعلومات الخاصة بالعميل إلا ضمن حدود الخدمات المالية المفتوحة التي تستدعي ذلك والمتفق عليها مع الشركة.

17. امتلاك خطط مناسبة لاستمرارية العمل والتعافي من الكوارث وبما يتناسب مع خطة استمرارية العمل والتعافي من الكوارث للشركة وفحصها وتحديثها بشكل دوري.

18. امتلاك سياسة امن المعلومات والأمن السيبراني وبما يتناسب مع سياسات الشركة.

19. الالتزام بسياسات وإجراءات التعرف والمصادقة على هوية العميل على ألا تقل عن مستوى الإجراءات المتبعة من قبل الشركة.

20. ضمان الفصل بين البيانات الخاصة بالخدمات المالية المفتوحة وعملائها والبيانات الخاصة به و/أو عملاءه الآخرين وتزويد الشركة بما يفيد بذلك.

21. إعلام الشركة فوراً عند حدوث أي عملية اختراق أو أية أحداث سلبية قد تؤثر على الشركة.

22. قيام مزود الطرف الثالث (TPP) بفحص الثغرات الأمنية على أنظمته فيما يخص العلاقة بينه وبين الشركة وتزويد الشركة بنتائجها.

23. في حال قيام مزود الطرف الثالث (TPP) بإسناد أي من عملياته تقنيًا -ضمن نطاق الخدمات المالية المفتوحة- لأطراف خارجية (outsourcing) ضمان قيامه بما يلي:

أ. إبلاغ الشركة بتفاصيل هذه العلاقة التعاقدية ونطاقها.
ب. تقديم الضمانات التي تؤكد بأن يقوم هذا الطرف الخارجي بالامتثال لبنود العلاقة التعاقدية بين الشركة ومزود الطرف الثالث (TPP).
ج. وجود خطة لاستمرارية العمل وفحصها بشكل دوري.
د. تطبيق الضوابط الأمنية والسيبرانية اللازمة لحماية البيانات وعدم تخزينها بأي شكل من الأشكال لديه.
ه. ضمان حقه بالمراقبة والتدقيق على الطرف الخارجي.

ب. مزود خدمة البدء بالدفع (PISP)

1. يجب أن يكون مزود خدمة البدء بالدفع (PISP) جهة مرخصة من البنك المركزي لممارسة نشاط خدمات الدفع والتحويل الإلكتروني للأموال في حال تقديمه خدمات إجراء عملية الدفع من خلاله بالنيابة عن العميل وأن تكون الخدمات التي سيقدمها بحدود الترخيص الممنوح له.
2. تحقيق كافة المتطلبات الوارد ذكرها في المادة (٩/أ) من هذه التعليمات.
3. أن يكون قادرًا على إجراء الاتصال الآمن لبدء الدفع لحساب العميل الدافع واستقبال جميع المعلومات الخاصة ببدء حركة الدفع وجميع المعلومات المتوفرة المتعلقة بتنفيذ الحركة لدى الشركة.
4. تزويد الشركة بنفس المعلومات المطلوبة من قبل العميل مستخدم الخدمات المالية المفتوحة عند بدء حركة الدفع مباشرة.
5. عدم حيازة/الاحتفاظ بأية أموال تخص عملاء الشركة في أي لحظة من اللحظات وبأي شكل من الأشكال باستثناء الشركات المرخصة لها الاحتفاظ بأموال العملاء من البنك المركزي.
6. وضع آليات لمراقبة عمليات الدفع التي تتم من خلاله لاكتشاف عمليات الدفع غير المصرح بها أو الاحتيال بغرض تنفيذ التدابير الأمنية، وضمان مراعاة آليات المراقبة للمخاطر المحتملة.
7. ضمان وصول كافة المعلومات الناشئة عن تقديم الخدمة لطرفي عملية الدفع فقط، بموافقة العميل الصريحة
8. عدم القيام بتعديل أية بيانات أو معلومات تم الحصول عليها لإتمام الخدمة من قبل العميل او الشركة الخاصة به.
9. عدم إمكانيه تغيير أي معلومات أو بيانات الخاصة بطلب حركة الدفع التي يتم إخطاره بها من قبل العميل.

المادة (١٠) المعايير الأمنية والفنية للخدمات المالية المفتوحة (Open Finance Standards)

يجب على الشركة تحديد وتوثيق المعايير اللازمة لتقديم الخدمات المالية المفتوحة اعتمادا على أفضل الممارسات في المجال وبحيث تشتمل المعايير بالحد الأدنى على ما يلي:

أ. **معايير هيكلة تصميم واجهة برمجة التطبيقات (Open API Standards)**

وهي المعايير التي تشتمل على بروتوكولات الاتصال (communication Protocols) ونوع هيكل التصميم (Architecture Type)، بحيث يتم تبني أساليب هيكلة معترف بها في مجال تطوير هذه الواجهات.

ب. **معايير البيانات (Data Standards)**

وهي المعايير الخاصة بصيغ البيانات (Data Format)، وهياكل البيانات (Data Structures) وقواعد حماية البيانات والخصوصية ذات الصلة، بحيث يتم تبني صيغ البيانات المعترف بها في المجال.

ج. معايير الأمن والحماية (Security Standards)

وهي المعايير التي تحدد الحد الأدنى من المتطلبات والمواصفات الأمنية التي يجب أن يفي بها المشاركون بما في الرجوع إلى الممارسات السليمة في هذا المجال والتعليمات والقوانين النافذة ذات الصلة وتطبيق الضوابط الأمنية والسيبرانية اللازمة وبما يتناسب مع المخاطر لحماية أنظمتهم وكذلك بيانات العملاء، وكحد أدنى يجب على المشارك تطبيق أحدث وأقوى برتوكولات التحقق والمصادقة (Authentication) التفويض والتخويل (Authorization) الكافية.

المادة (١١) حماية المستهلك (Consumer protection) وخصوصية البيانات وحماية البيانات (Data Privacy and data protection)

أ. يجب على الشركة اخذ التدابير اللازمة لتوعية عملائها بالحد الأدنى بما يلي:

1. حماية معلومات.
2. الخدمات المالية المفتوحة.
3. العمولات والتكاليف الفعلية المتعلقة بالوصول إلى البيانات و/أو المعلومات وتنفيذ المعاملات المالية.
4. أحكام وشروط الخدمات المالية المفتوحة.
5. المنتجات والخدمات المناسبة له.
6. إجراءات حل المشاكل المتعلقة بالخدمات المالية المفتوحة.

ب. يجب على الشركة الإفصاح لعملائهم وقبل الشروع بأي خدمة من الخدمات المالية المفتوحة عن جميع المخاطر المحتملة بطريقة واضحة وعادلة وغير مضللة وبشكل مستمر.

ج. على كل شركة القيام بنشر قائمة بمزودي الأطراف الثالثة (TPP) الذين يشترك معهم والمنتجات والخدمات ذات الصلة التي سيقدمونها وتحديثها باستمرار.

د. يجب أن يحتوي كل عقد يتعلق بتنفيذ أو استخدام الخدمات المالية المفتوحة وواجهة برمجة التطبيقات على بند للإقرار من قبل كل طرف بأن حق المشاركين في التحكم في استخدام هذه البيانات يقتصر على حدود موافقة العميل الصريحة.

ه. يجب على المشاركين وضع آليات مناسبة لضمان عدم استخدام البيانات و/أو المعلومات الخاصة للعملاء لأغراض تتعارض مع مصالح هؤلاء العملاء. بحيث يجب الاستمرار بأخذ موافقة العميل الصريحة على كيفية استخدام بياناتهم وتزويدهم بآليات إلغاء الموافقة إذا أرادوا الانسحاب أو تعديل نطاقها.

و. يجب على الشركة توفير بوابة أو منصة لخدمة إدارة موافقات العملاء بناء على أفضل الممارسات بالخصوص وذلك لتسجيل الموافقات التي تم الحصول عليها والفترة الزمنية لها والخدمات التي تم قبول / إلغاء الاشتراك فيها وغيرها من الأمور ذات العلاقة.

ز. يجب أن يكون لدى المشـــاركين آلية أو إجراء مناســـب وفق التشـــريعات الصـــادرة عن البنك المركزي بالخصـــوص للتعامل مع النزاعات المتعلقة بالخدمات المالية المفتوحة وحلها (Dispute Resolution Mechanism).

ح. يجب على الشركة ضمان قيام مزود الطرف الثالث (TPP) بالإفصاح للعملاء عما يلي:

1. الاسم التجاري والعنوان وتفاصيل الاتصال الخاصة بمزود الطرف الثالث (TPP) حسب الحالة.
2. وصف الخصائص الرئيسية للخدمة المالية المفتوحة التي سيتم تقديمها.
3. المعلومات أو المعرف الخاص به الذي يجب أن يقدمه العميل من أجل استخدام الخدمات المالية المفتوحة.
4. شكل وإجراءات منح موافقة العميل الصريحة لتقديم خدمة معلومات الحساب، وخدمة الشروع (البدء) الدفع وسحب الموافقة والتعديل عليها.
5. الأحكام المتعلقة بوقت والمدة القصوى لتنفيذ خدمة الدفع التي يتعين تقديمها أن وجد.
6. سقوف الحركات إن وجدت.
7. تفاصيل جميع الرسوم والعمولات التي يدفعها العميل إلى مزود الطرف الثالث (TPP).
8. وسائل الاتصال المتفق عليها بين العميل ومزود الطرف الثالث (TPP) فيما يتعلق بإرسال المعلومات والإشعارات.
9. الشروط التي يجوز للعميل بموجبها الانسحاب من الخدمة التي يوفرها مزود الطرف الثالث (TPP) إن وجدت.

ط. يجب على الشركة ضمان قيام مزود الطرف الثالث (TPP) بالإفصاح عن المعلومات التالية حول الإجراءات الوقائية والتدابير التصحيحية للعميل عند التعاقد مع العميل:

1. وصـــف للخطوات التي يجب على العميل اتخاذها من أجل الحفاظ على أمان الخدمات المالية المفتوحة وكيفية إخطار مزود الطرف الثالث (TPP) فيما يتعلق بالفقد والسرقة والاختلاس.
2. الإجراءات الآمنة، التي من خلالها ســـيتصـــل مزود الطرف الثالث (TPP) بالعميل في حالة الاحتيال المشتبه به أو الفعلي أو التهديدات الأمنية.
3. الشروط التي بموجبها يقوم مزود الطرف الثالث (TPP) بإيقاف أو منع استخدام الخدمات المالية المفتوحة.
4. مسؤولية العميل.
5. مسـؤولية الأطراف المشـاركة بخصـوص تنفيذ أو تأخير تنفيذ أو عدم تنفيذ الخدمات المالية المفتوحة وفي حال حدوث حدث سيبراني.

6. كيف وفي أي فترة زمنية يقوم العميل بإخطار الشـــركة التي تحتفظ بحســـاب العميل بأي معاملة دفع غير مصـــرح بها أو بدأت أو نفذت بشـــكل غير صـــحيح، والمســـؤولية، إن وجدت، عن معاملات الدفع غير المصرح بها التي تقع على عاتق الشركة التي تحتفظ بحساب العميل لتنفيذ غير مصرح به.

7. أحكام إنهاء التعاقد.

المادة (١٢) الفحص والاختبار

تقوم الشركة بإعداد قائمة بحالات الاستخدام (Use Cases) للخدمات المالية المفتوحة مع تحديد المعايير الفنية والأمنية المطلوبة من مزودي الطرف الثالث والتأكد من قيام مزود الطرف الثالث (TPP) بتنفيذ فحوصـات الأمنية والفنية والوظيفية المتعلقة بالخدمات المالية المفتوحة المقدمة.

المادة (١٣): أحكام عامة

أ. للبنك المركزي في أي وقت الحق بطلب إنهاء التعاقد الذي أجرته الشـــركة مع مزود الطرف الثالث (TPP) كلياً أو جزئياً بشكل فوري أو وفقاً لما يراه مناسباً.

ب. للبنك المركزي إصـــدار أوامر لتحديد الحد الأدنى والأعلى لعمولات التي تتقاضـــاها الشـــركات في منظومة الخدمات المالية المفتوحة.

ج. تلتزم كافة الشـــركات بإتاحة الخدمات المالية المفتوحة من خلال التعاقد مع مزود الطرف الثالث (TPP) في حال تلبيته لكافة المتطلبات الواردة في هذه التعليمات.

د. مع عدم الإخلال بمسؤولية مزود الطرف الثالث تكون الشركة المسؤولة بالكامل تجاه البنك المركزي عن كافة أعمال مزود الطرف الثالث (TPP) بحدود الخدمات المالية المفتوحة المقدمة من قبله بما في ذلك امتثاله لأحكام هذه التعليمات وأية تعليمات أو تعاميم تصدر لاحقا بالخصوص.

المحافـــــظ

د. عادل الشركس