مصرف ليبيا المركزي

ص.ب 1103 العنوان البرقي : مصرفليبيا ـ طرابلس ـ ليبيا

الإشاري /804 ( )

منشور ا ر م ن رقم (18 /2025)
التاريخ : 6 محرم 1447 هـ
الموافق : 2025/7/1

السادة / المـــدراء العامين للمصارف
السـادة / المدراء العامين للمصـارف المتخصصة
(التنمية – الزراعي – الريفي - الادخار الاستثمار العقاري)
السادة / شركة معاملات للخدمات المالية
السادة / شركات الدفع الإلكتروني المرخص لها من قبل مصرف ليبيا المركزي
بعد التحية ،،،

الموضوع: "**نظام حماية البيانات و اللائحة التنظيمية لحماية البيانات و المعلومات للقطاع المصرفي** "

تأسيساً على أحكام القانون رقم (1) لسنة 2005، بشأن المصارف وتعديلهِ و قانون مُكافحة غسل الأموال و تمويل الإرهاب رقم (1013) لسنة 2017، وعلى الدور الإشرافي والرقابي الذي يُمَارِسهُ مصرف ليبيا المركزي على كافة المصارف العاملة بليبيا وفقاً لأحكام القانون .

و بالإشارة إلى المنشور ا ر م ن رقم (2024/10) المؤرخ في 2024/5/19. الذي أُحيل بموجبه ضوابط مكافحة غسل الأموال و تمويل الإرهاب لشركات الدفع الإلكتروني .

و إلى المنشور ا ر م ن رقم (2024/21) المؤرخ 2024/12/4، بشأن العمل على إتخاذ الإجراءات اللازمة بشأن تفعيل البطاقات المصرفية على منصة التجارة الإلكترونية مع تسهيل إجراء التعاقد مع اصحاب منصات التجارة على شبكة المعلومات الدولية (الإنترنت) وذلك وفقاً للمعايير المطلوبة لأمن و سلامة المعلومات .

و إلى المنشور ا ر م ن رقم (2025/7) المؤرخ في 2025/2/20. بشأن التأكيد على ضرورة إبلاغ مالكي بطاقات الدفع المسبق بعدم منح البطاقات الممنوحة لهم للغير حتى لا يتم استعمالها في أنشطة مشبوهة ذات صلة بغسل الأموال و تمويل الإرهاب .

و إلى المنشور ا ر م ن رقم (2025/8) المؤرخ في 2025/3/3، بشأن مكافحة الإحتيال و متطلبات الأمن و السلامة لأجهزة الصراف الآلي (ATM"S) .

عليه نحيل إليكم نظام حماية البيانات و اللائحة التنظيمية لحماية البيانات و المعلومات للقطاع المصرفي، لِوضع ما جاء به موضع التنفيذ وفق آلية التطبيق الواردة باللائحة .

والسلام عليكم

عبدالمجيد محمد الماقوري
مُدير إدارة الرقابة على المصارف والنقد

صورة للسيد/ المحافظ
صورة للسيد/ نائب المحافظ
صورة للسيد/ مدير إدارة البحوث و الإحصاء – مصرف ليبيا المركزي
صورة للسيد/ مدير وحدة المعلومات المالية الليبية – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة تقنية المعلومات – مصرف ليبيا المركزي
صورة للسيد/ مدير إدارة الحسابات - مصرف ليبيا المركزي
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف و النقد
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد لشؤون الرقابة المكتبية ومتابعة الامتثال
صورة للسيد/ نائب مدير إدارة الرقابة على المصارف والنقد للشؤون الرقابة المصرفية - بنغازي
صورة للسادة مدراء وحدات الامتثال بالمصارف
صورة لقسم المتابعة المصرفية و مراقبة الامتثال
ك/ ن. ايجاد ✓/ منشور 2025

مصرف ليبيا المركزي
CENTRAL BANK OF LIBYA

اللائحة التنظيمية لحماية البيانات الشخصية

اللائحة التنظيمية لحماية البيانات الشخصية

الفصل الأول: الأحكام العامة

المادة (1) التعريفات

في تطبيق أحكام هذا النظام يكون للألفاظ والعبارات التالية المعاني المقابلة لها ما لم يدل سياق النص على غير ذلك:

الجهة المختصة: مصرف ليبيا المركزي.

المؤسسة المالية: هي الجهة المرخص لها من قبل الجهة المختصة بالاحتفاظ بالحسابات و/أو منح الائتمان و/أو التعامل في التحويلات المالية أو الدفع الالكتروني.

مقدم خدمة الدفع الإلكتروني: هو الجهة المرخص لها من قبل الجهة المختصة لتقديم خدمات الدفع الإلكتروني.

البيانات الالكترونية: هي بيانات ومعلومات ذات خصائص إلكترونية في شكل نصوص، أو رموز، أو أصوات، أو رسوم، أو صور، أو برامج الحاسوب، أو غيرها من أشكال تعتمد على التمثيل الإلكتروني.

البيانات الشخصية: هي كل بيان من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنا بصفة مباشرة، أو غير مباشرة، مثل: الاسم، الرقم الوطني، رقم ورقة العائلة، رقم قيد العائلة، رقم الهاتف، العنوان، رقم الهوية الشخصية، الصور الشخصية، صور المستندات الشخصية، البريد الالكتروني، الإقامة للأجانب وغير ذلك من البيانات ذات الطابع الشخصي.

بيانات الشركات: ويقصد بها الجهات الاعتبارية سواءً عامة أو خاصة مثل: رقم العميل، رقم الحساب، رصيد الحساب، العمليات على الحساب، الرمز الإحصائي، النظام الأساسي، السجل التجاري، الترخيص التجاري، رسالة الإشهار، هيكلة الملكية.

البيانات المالية: رقم العميل، رقم الحساب (محلي او دولي)، رصيد الحساب، العمليات على الحساب، بيانات البطاقة المصرفية (محلية أو دولية)، البيانات الائتمانية، بيانات المحافظ الالكترونية، الحوالات، بيانات الدفع (سواءً الدافع أو المدفوع له أو طريقة الدفع)، أرقام الدفاتر، ويجب التعامل مع أي معلومات شخصية مرتبطة ببيانات الشركات مثل بيانات الإتصال للموظفين أو الملاك وفقا لأحكام حماية البيانات الشخصية.

البيانات الائتمانية: كل بيان شخصي لفرد أو لشخص إعتباري يتعلق بطلب الفرد الحصول على تمويل أو حصوله عليه من جهة تمارس التمويل، بما في ذلك أي بيانات تتعلق بقدرته على الحصول على ائتمان أو بقدرته على الوفاء به وبتاريخه الائتماني.

البيانات: وتشمل البيانات الشخصية، وبيانات الشركات، والبيانات المالية، والبيانات الإئتمانية.

البيانات الحساسة: هي فئة خاصة من البيانات الشخصية تتطلب حماية إضافية نظراً لطبيعتها الحساسة والمخاطر العالية المرتبط بمعالجتها وتشمل على سبيل المثال لا الحصر (البيانات الصحية، البيانات الوراثية، البيانات البيومترية).

صاحب البيانات الشخصية: الفرد الذي تتعلق به البيانات الشخصية.

الولي الشرعي: الشخص الذي يمثل القاصر، أو المحجور عليه لدى المحاكم وينوب عنه في جميع الاعمال القانونية والتصرفات المالية.

الأموال: هي الأصول أو الممتلكات أيًا كان نوعها سواء كانت مادية، أو غير مادية، ملموسة، أو غير ملموسة، منقولة، أو ثابتة أيًا كانت طريقة الحصول عليها، وكافة الحقوق المتعلقة بها، وجميع المستندات أو الوثائق المثبتة لحق ملكيتها أو ملكية حصةٍ فيها أيًا كان شكلها، بما في ذلك المستندات الالكترونية أو الرقمية وتشمل على سبيل المثال لا الحصر:

1- النقود بالعملات المحلية والأجنبية والعملات الافتراضية والالكترونية وأرصدة الحسابات المصرفية.
2- الأوراق التجارية.
3- الاعتمادات المصرفية.
4- الصكوك السياحية.
5- الحوالات المالية والأوراق المالية كالأسهم والسندات والاعتمادات المستندية والمستندات برسم التحصيل وبوالص التأمين.
6- الكمبيالات.

المحفظة الالكترونية: هي حساب يحتوي على قيمة النقود الالكترونية يمتلكه العميل في شركات الدفع الالكتروني.

أنظمة الدفع الالكترونية: هي مجموعة البرمجيات أو الترتيبات أو إجراءات التشغيل ونظم المعلومات وشبكات الاتصال المعدة للدفع أو التحويل أو التقاص أو التسويات للأموال إلكترونيا وبأي عملة كانت، وتنقسم الى:

-أنظمة مدفوعات التجزئة.

-أنظمة الدفع عالية القيمة.

-أنظمة تسوية الأوراق المالية.

-أنظمة التحويل المالي وصرف العملات الأجنبية.

أدوات الدفع: كل أداةٍ تمكن المستخدم من الحصول على الأموال والسلع والخدمات أو القيام بعمليات الدفع وتحويل الأموال.

خدمات الدفع الإلكتروني: هي الخدمات المتعلقة بإدارة النقود الإلكترونية، أي المبالغ التي يتم تداولها إلكترونيا، وكذلك الخدمات المتعلقة بإصداروإدارة أي من أدوات الدفع المدفوعة مسبقاً، أو أي أعمال أخرى تتضمن الحصول على الأموال والسلع والخدمات التي تقرر الجهة المختصة إخضاعها لأحكام هذه التعليمات وذلك بموجب أوامر خاصة تصدرها الجهة المختصة لهذه الغاية.

النقود الإلكترونية: هي قيمة نقدية مستحقة على الطرف الذي قام بإصدارها، وتكون مخزنة إلكترونيا أو مغناطيسيا أو أي وسيلة أخرى، وتصدر مقابل إستلام نقد حقيقي مقابلها يتم إيداعه في حسابات التسوية في المصارف التجارية بغية تنفيذ عمليات الدفع الإلكتروني وتكون وسيلة دفع مقبولة في ليبيا.

البطاقة المالية الإلكترونية: هي وسيط إلكتروني مادي أو افتراضي يستعمل في عمليات السحب أو الإيداع أو الدفع الإلكتروني باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات.

التشفير: هو عملية تحويل البيانات الإلكترونية إلى رموز غير معروفة أو غير مفهومة يستحيل قراءتها أو معرفتها دون إعادتها إلى هيأتها الأصلية.

النشر: بث أي من البيانات الشخصية عبر وسيلة نشر مقروءة أو مسموعة أو مرئية.

المستند القانوني: هو وثيقة توضح حقوق صاحب البيانات ويمكن أن تكون ورقية أو إلكترونية.

قنوات التواصل الرسمية: وهي القنوات التي يتم بها التواصل بين صاحب البيانات وبين المؤسسة المالية، وهي البريد الإلكتروني الموثق، والبوابة الإلكترونية للمؤسسة المالية، والحضور الشخصي لصاحب البيانات لمقر المؤسسة المالية.

المادة (2)

الهدف من اللائحة

تهدف أحكام هذه اللائحة لوضع الضوابط والشروط والإجراءات التنظيمية اللازمة لتنفيذ نظام حماية البيانات الصادر من مصرف ليبيا المركزي بما يضمن الشفافية والعدالة في معالجة هذه البيانات، ويعزز الثقة في التعاملات المالية، ويحقق التوازن بين المصالح المشروعة وحقوق الأفراد في حماية خصوصيتهم.

المادة (3)

تحديد نطاق البيانات

تحدد اللائحة بشكل واضح البيانات التي تقع في نطاق النظام وهي البيانات الشخصية وبيانات الشركات والبيانات المالية والبيانات الإئتمانية والبيانات التي يمكن أن تتفرع من هذه البيانات أيضا ويمكن للمؤسسة أن تدخل أي بيانات ترى أنها حساسة بشكل خاص وتتطلب حماية إضافية أخرى في نطاق النظام وذلك لرفع مستوى حماية البيانات في المؤسسة.

المادة (4)

نطاق تطبيق النظام

تُسري أحكام هذه اللائحة على جميع المؤسسات المالية المنصوص عليها في النظام، وتُشكل مرجعًا تفصيليًا لتحديد الإجراءات والالتزامات العملية، بما في ذلك أنواع البيانات التي تُجمع، وتُعالج، وتُخزن، وخاصة البيانات الحساسة التي تتطلب حماية إضافية، وتشمل المؤسسات الأتية:

1- مصرف ليبيا المركزي.
2- المصارف الليبية.
3- فروع ومكاتب المصارف الأجنبية وشركات الخدمات المالية العاملة في ليبيا.
4- شركات الدفع الالكتروني.
5- شركات الصر افة المالية.
6- المؤسسات أو الشركات التي تمنح الائتمان.
7- شركات التأجير التمويلي.

يمكن للجهة المختصة إضافة أية مؤسسات إضافية في المستقبل.

المادة (5)

أحقية جمع البيانات

أولاً: يجب أن تقوم المؤسسة المالية بتوفير مستند قانوني لصاحب البيانات يوضح له الغرض من جمع البيانات وطريقة جمع ومعالجة البيانات وحقوقه وقنوات التواصل الرسمية التي يمكنه أن يقوم باستعمالها للتواصل مع المؤسسة المالية.

ثانياً : يجب أن تقوم المؤسسة بتصنيف البيانات التي تريد جمعها كبيانات أساسية أو بيانات إضافية.

البيانات الأساسية هي التي لا يمكن تقديم الخدمة لصاحب البيانات إلا بوجودها وتعتبر إلزامية أما البيانات الإضافية فهي بيانات تساعد المؤسسة في عملها، ولكن يمكن تقديم الخدمة بدونها ويعتبر تقديمها من طرف صاحب البيانات إختياريا.

ثالثاً : لا يمكن أن تشترط المؤسسة على صاحب البيانات تزويدها بالبيانات ليتم تقديم الخدمات له إلا إذا كان تصنيف هذه البيانات بيانات أساسية ولا يمكن أن تقدم الخدمة بدونها.

الفصل الثاني

جمع البيانات

المادة (6)

خطوات جمع البيانات

تقوم المؤسسة بإعداد نموذج لجمع البيانات يتضمن نوعها، الغرض من جمعها، وبيان إلزاميتها أو اختياريتها، ويجب توثيق الجمع عبر سجلات إلكترونية غير قابلة للتعديل بعد التسجيل تحتوي على:

1- الغرض من جمع البيانات.
2- اسم الموظف المسؤول عن جمع البيانات.
3- وصف للبيانات التي يتم جمعها.
4- توقيع صاحب البيانات.
5- تاريخ ووقت جمع البيانات.
6- قناة جمع البيانات.

المادة (7)

قنوات جمع البيانات (القنوات الرسمية)

تتم عبر:

1- الحضور الشخصي لصاحب البيانات بشكل مباشر، أو من له الولاية الشرعية عليه ومن غير وجود وسيط لمقر المؤسسة أو أحد فروعها.
2- البوابة الإلكترونية للمؤسسة.
3- البريد الإلكتروني الموثق.

مع تحديد وسيلة تواصل مع مسؤول البيانات لأي طلب متعلق بالبيانات وعلى ان تكون وسائل التواصل الإلكتروني آمنة وموثوقة.

المادة (8)

طرق المو افقة

يجب الحصول على مو افقة مسبقة حرة ومحددة وغير غامضة ويمكن إثباتها عند الطلب وصريحة موثقة عبر:

1- توقيع سواءً أكان ورقي (حضوريا)، أو إلكتروني آورقمي (عن بعد).
2- المو افقة عن طريق التطبيقات الرقمية بشرط أن تكون معتمدة على المصادقة البيومترية سواءً كانت بصمة الإصبع، أو التعرف على الوجه، ويتم الاحتفاظ بنسخة من المو افقة في سجلات إلكترونية.
3- صوتية في حالة تسجيل المكالمات.

المادة (9)

ضو ابط المو افقة

لا يُعتد بالمو افقة الضمنية إلا وفق ضو ابط قانونية محددة وبمو افقة من مسؤول البيانات، ويجب توثيق جميع وسائل المو افقة المستخدمة ويجب أن تكون المو افقة منفصلة عن أي شروط أو بنود أخرى، كما يجب إعلام صاحب البيانات بحقه في سحب المو افقة في أي وقت، وأن سحب المو افقة لا يؤثر على شرعية التعاملات التي تمت قبل السحب.

في حالة سحب المو افقة، يجب على المؤسسة التوقف عن معالجة البيانات التي تستند إلى هذه المو افقة مع مراعاة أي إشتراطات قانونية تستلزم الإحتفاظ بالبيانات.

المادة (10)

تقليل البيانات والأساس القانوني

يجب جمع الحد الأدنى من البيانات اللازمة فقط، وتوثيق الأساس القانوني لكل عملية جمع في سجل داخلي.

المادة (11)

التصحيح والتحديث

يجب على المؤسسة المالية توفير آلية واضحة وميسرة لصاحب البيانات لطلب تصحيح أو تحديث بياناته الشخصية، والمالية، ويجب عليها الإستجابة لهذا الطلب في غضون 15 يوماً من تاريخ إستلام الطلب، مالم تكن هناك ظروف استثنائية تستدعي تمديد الفترة، وفي جميع الأحوال يجب إعلام صاحب البيانات بسبب التأخير والمدة المتوقعة للإستجابة مع توثيق العملية في النظام الإلكتروني.

المادة (12)

حقوق صاحب البيانات

يشمل ذلك: الاطلاع، التصحيح، الحذف، الاعتراض، ونقل البيانات لجهة أخرى، ضمن الإمكانيات التقنية المتوفرة مع مراعاة أي إلتزامات قانونية أخرى تفرضها جهات مختصة قانونية تستلزم الإحتفاظ بالبيانات.

الفصل الثالث

معالجة البيانات.

المادة (13)

ضوابط المعالجة

أ) يجب أن تكون جميع عمليات معالجة البيانات الشخصية، والمالية، عادلة وشفافة وقانونية.
ب) يجب أن تتم المعالجة لأغراض محددة ومشروعة.
ت) يجب أن لا تتعدى المعالجة الغرض الذي جمعت من أجله البيانات.
ث) يجب الحفاظ على دقة البيانات.
ج) يجب دعم حماية معالجة البيانات بشكل إستباقي بدءً من مراحل تصميم النظم مرورا بالتطوير وكذلك الخدمات.

المادة (14)

التغييرات في البيانات

يتم إبلاغ صاحب البيانات بأي تعديل جوهري يتم على بياناته عبر القنوات الرسمية ومسببات التغيير سواءً أكانت قانونية أو لضرورة تعاقدية.

المادة (15)

ضوابط الخصوصية

يجب تطبيق ضوابط الخصوصية الإدارية مثل:

1- سياسة تصنيف البيانات.
2- سياسية خصوصية البيانات.
3- سياسة معالجة البيانات.
4- سياسة إدارة الوصول.

5- سياسة التشفير.
6- سياسة إدارة الثغرات.
7- سياسة الإستجابة للحوادث الأمنية.
8- سياسة الإحتفاظ بالمعلومات والإتلاف الأمن.

يمكن دمج هذه السياسات داخل السياسات الموجودة في المؤسسة من قبل.

وضوابط الخصوصية التقنية مثل:

1- نظام مراقبة السجلات (نظام يقوم بمراقبة السجلات والملفات ويحدد أي تغيير قد تم عليها)
2- نظام إدارة الوصول.

الفصل الرابع

تخزين البيانات

المادة (16)

البنية الأساسية للتخزين

يجب أن تكون البيانات محفوظة داخل الدولة الليبية في مراكز بيانات معتمدة من قبل الجهة المختصة، وتحت إشراف أمن معلوماتي متكامل ويلتزم بأعلى معايير الأمن السيبراني وحماية البيانات ويشترط الحصول على شهادة PCIDSS لضمان حد أدنى من الحماية.

المادة (17)

الاستضافة المحلية المشروطة

يجوز استضافة البيانات داخل ليبيا بشرط وجود اتفاقية مستوى خدمات (SLA) تشمل البنود الأمنية والاحترازية بعد إعتمادها من قبل الجهة المختصة و أيضا يشترط الحصول على شهادة PCIDSS لضمان حد أدنى من الحماية ويجب على المؤسسات المالية التدقيق الدوري من إمتثال مزودي الخدمات لهذه المعايير.

المادة (18)

حظر النقل الخارجي

يُمنع منعًا باتًا نقل البيانات الشخصية أو المالية أو الائتمانية خارج الدولة الليبية.

المادة (19)

التشفير وحماية البيانات

يجب تطبيق التشفير المتقدم، وإدارة مفاتيح التشفير بشكل مستقل، وتطبيق تقنيات التشفير على كل الأنظمة التي تحتوي على البيانات وخاصة قواعد البيانات، الخاصة بالمؤسسة ويكون التشفير دائم سواء عند التخزين، أو نقل البيانات، ولا يسمح بوجود مفاتيح التشفير في نفس المكان الذي توجد به البيانات.

المادة (20)

الضوابط الإدارية والتقنية

يُشترط توفر سياسات إدارية مثل:

1- سياسة أمن المعلومات.
2- سياسة تقييم المخاطر.
3- سياسة الحماية المادية.
4- سياسة إدارة مفاتيح التشفير.
5- سياسة سجلات الوصول.
6- سياسة إدارة الصلاحيات.
7- سياسة النسخ الإحتياطي.
8- خطط استمرارية العمل والتعافي من الكوارث.
9- إلتزام جميع الموظفين بسياسة سرية البيانات بتوقيع إتفاقية عدم الإفصاح.

يمكن دمج هذه السياسات داخل السياسات الموجودة في المؤسسة من قبل.

وكذلك أنظمة تقنية مثل:

1- أنظمة إدارة الهوية.
2- أنظمة إدارة الصلاحية.
3- أنظمة المصادقة الثنائية.
4- أنظمة النسخ الإحتياطي.
5- أنظمة مراقبة وتسجيل الأحداث.
6- أنظمة إدارة التحديثات الأمنية الدورية للأنظمة والتطبيقات.

المادة (21)

إدارة البيانات الحساسة

تتطلب البيانات الحساسة حماية مشددة، عبر:

1- تقييد الوصول.
2- توثيق المعالجة بسجلات منفصلة.
3- تشفير إلزامي.
4- الحصول على موافقة صريحة لمعالجة البيانات الحساسة، إلا في الحالات التي ينص فيها القانون على خلاف ذلك.

المادة (22)

الالتزامات التعاقدية لمزودي الخدمة

في حالة الإعتماد على مزود خدمة محلي لاستضافة البيانات تُلزم المؤسسة مزودي الخدمة عند التعاقد بتطبيق والإمتثال لمعايير الأيزو مثل 27001/27701 و PCIDSS، والإلتزام بحماية البيانات، والتبليغ عن الحوادث في مزود الخدمة، وتحديث اتفاقيات مستوى الخدمة (SLA) بشكل دوري وحظر معالجة البيانات دون موافقة مسبقة من المؤسسة المالية، مع إلزامه بإبلاغ المؤسسة المالية فور حدوث خرق أمني، مع تحديد مسؤوليات واضحة للأطراف في حال عدم الإمتثال أو حدوث خرق وتحديد شروط إعادة البيانات أو إتلافها عند إنتهاء العقد.

الفصل الخامس

تقييم الأثر على الخصوصية

المادة (23)

الحالات التي يستلزم فيها إجراء التقييم

يجب على المؤسسة المالية إجراء تقييم الأثر على الخصوصية بشكل دوري كل ستة أشهر، و أيضا في أي من الحالات الآتية:

1- إنشاء خدمات مالية إلكترونية جديدة، أو تحديث جوهري في الخدمات القائمة.
2- البدء في جمع، أو معالجة بيانات حساسة جديدة، أو بطرق غير مسبوقة.
3- استخدام تقنيات قد تؤثر بشكل كبير على خصوصية الأفراد، مثل الذكاء الاصطناعي أو المصادقة البيومترية.
4- مشاركة البيانات مع أطراف خارجية، أو نقل البيانات بين أنظمة، أو قواعد بيانات مختلفة.
5- تنفيذ أنشطة تتضمن مراقبة منهجية، أو واسعة النطاق للمستخدمين.

المادة (24)

خطوات التقييم

يتعين على المؤسسة المالية إعداد وثيقة رسمية لتقييم الأثر على الخصوصية تتضمن على الأقل ما يلي:

1- وصف النشاط، أو النظام، أو الخدمة موضوع التقييم.
2- تحديد أنواع البيانات التي ستتم معالجتها والغرض من جمعها.
3- تحديد الأشخاص المعنيين بالبيانات (أفراد، شركات...).
4- تحديد وتقييم المخاطر المحتملة على خصوصية أصحاب البيانات.
5- عرض التدابير الفنية والإدارية المقترحة للحد من تلك المخاطر.
6- رأي مسؤول البيانات في جدوى المعالجة وأمانها.
7- الاحتفاظ بنتائج التقييم في سجل خاص، و إتاحته للجهة المختصة عند الطلب.

المادة (25)

المسؤولية عن التقييم

يُعد تقييم الأثر على الخصوصية مسؤولية مشتركة بين الوحدة المنفذة داخل المؤسسة المالية ومسؤول البيانات.

يُعتمد التقييم من الإدارة العليا قبل تنفيذ المشروع أو التغيير محل التقييم.

المادة (26)

مراجعة وتحديث التقييم

يتم تحديث تقييم الأثر في الحالات التالية:

1- حدوث تغيير جوهري في آليات المعالجة.
2- اكتشاف مخاطر جديدة بعد التشغيل.
3- تحفظ نسخة من أي تقييم محدَّث مع بيان التعديلات وأسبابها.

الفصل السادس

إدارة حوادث البيانات

المادة (27)

يجب أن توجد لدى المؤسسة سياسة أو خطة خاصة بإدارة حوادث البيانات وتشمل على كل الإجراءات التي يجب القيام بها عند حصول أي حادث على أن تشمل (إجراءات الكشف عن الحوادث والتحقق منها، إجراءات الإحتواء والتخفيف من الآثار، إجراءات التحقيق في سبب الحادث، إجراءات التعافي) ورفع تدابيروقائية لمنع التكرار.

المادة (28)

يجب أن يتم التدريب على خطة أو سياسة إدارة الحوادث والتأكد من فعاليتها كل ستة أشهر على الأقل ويكون موثق.

المادة (29)

يجب إبلاغ الجهة المختصة فوريا عند حدوث أي تسريب أو وصول غير مشروع للبيانات خلال 24 ساعة، مع إشعار صاحب البيانات في حالة حدوث تسرّب أو تلف لبياناته أو حدوث وصول غير مشروع إليها، وإذا كان من شأن حدوث أياً مما سبق أن يرتب ضرراً جسيماً على بياناته أو على نفسه، فيجب على المؤسسة المالية إبلاغه فوراً ، وتوثق جميع الحوادث والإجراءات التصحيحية ويكون مسؤول البيانات هو المسؤول عن هذا الإجراء ويتحمل المسؤولية ويجب أن يتضمن الإبلاغ للجهة المختصة حد أدنى (طبيعة الخرق الأمني، والفئات والأنواع من البيانات المتأثرة، بيانات مسؤول البيانات ومعلومات التواصل، العو اقب المحتملة للخرق الأمني، الإجراءات المتخذة أو المقترح إتخاذها للمعالجة أو التخفيف من آثار الخرق الأمني.

الفصل السابع

إزالة و إتلاف البيانات

المادة (30)

تتم الإزالة بناءً على طلب رسمي من صاحب البيانات أو من مسؤول البيانات، وبعد التحقق من انتهاء الغرض من الاحتفاظ وبما لا يتعارض مع القانون.

المادة (31)

يُستخدم الإتلاف الآمن التقني (مثل الحذف المغناطيسي)، ويُوثق تاريخ الإتلاف، نوع البيانات، والمسؤول عن العملية في سجل خاص.

الفصل الثامن

مسؤول البيانات

المادة (32)

مسؤول البيانات هو شخص يتم تعيينه في إدارة الإمتثال في المؤسسة المالية، ويقدم تقارير إلى الإدارة العليا ويشرف على الامتثال للنظام.

المادة (33)

يكون مسؤول البيانات هو الشخص المسؤول والمحاسب أمام القانون والجهة المختصة.

المادة (34)

يكون مسؤول البيانات ليبي الجنسية، ويتم الموافقة على تعيينه من قبل الجهة المختصة بعد إرسال المؤسسة المالية لملفه.

المادة (35)

يتولى مسؤول البيانات المسؤوليات الآتية:

1- العمل كمسؤول اتصال مباشر مع الجهة المختصة، وتنفيذ قراراتها فيما يخص البيانات.
2- الإشراف على إجراءات المراجعة والتدقيق وتقييم الأثاروتوثيق نتائج التقييم وإصدار التوصيات اللازمة.
3- تمكين صاحب البيانات من ممارسة حقوقه.
4- إشعار الجهة المختصة عن حوادث التسريب.
5- الإشراف على معالجة المخالفات داخل المؤسسة المالية.
6- الرد على الطلبات المقدمة من صاحب البيانات والجهة المختصة.
7- متابعة قيد وتحديث سجلات أنشطة المعالجة.
8- يتولى إعداد التقارير الخاصة بالجهة المختصة.
9- الإشراف على خطط التدريب المتعلقة بحماية البيانات وخصوصيتها.
10- ضمان توثيق جميع عمليات معالجة البيانات وفقا للائحة.
11- المساهمة في التحقيق في أي خروقات أمنية وتقديم التوصيات لمنع تكرارها.

الفصل التاسع

التقييم الدوري والإلتزام.

المادة (36)

تُجري المؤسسة تقييمًا سنويًا لمدى الالتزام بالنظام، وتوثق نتائج التقييم ويتم إرسال هذه النتائج كتقرير سنوي إلى الجهة المختصة.

المادة (37)

تنفذ برامج تدريب إلزامية للعاملين، مع مراجعة فهم الموظفين عبر اختبارات سنوية وتحفظ النتائج في سجلات.

الفصل العاشر

العقوبات

المادة (38)

يُعاقب كل من يخالف أحكام هذه اللائحة بغرامة مالية قدرها مئة ألف دينار ليبي، عن كل مخالفة، وذلك استناداً للقانون رقم (1) لسنة 2005، بشأن المصارف وتعديله، بالإضافة إلى أية عقوبات أخرى تفرضها الجهة المختصة وفقاً لصلاحياتها.

مصرف ليبيا المركزي

CENTRAL BANK OF LIBYA

نظام حماية البيانات

نظام حماية البيانات

المادة الأولى

التعريفات:

في تطبيق أحكام هذا النظام يكون للألفاظ والعبارات التالية المعاني المقابلة لها ما لم يدل سياق النص على غير ذلك:

الجهة المختصة: مصرف ليبيا المركزي.

المؤسسة المالية: هي الجهة المرخص لها من قبل الجهة المختصة بالاحتفاظ بالحسابات و/أو منح الائتمان و/أو التعامل في التحويلات المالية أو الدفع الالكتروني.

مقدم خدمة الدفع الإلكتروني: هو الجهة المرخص لها من قبل الجهة المختصة لتقديم خدمات الدفع الإلكتروني.

البيانات الالكترونية: هي بيانات ومعلومات ذات خصائص إلكترونية في شكل نصوص، أو رموز، أو أصوات، أو رسوم، أو صور، أو برامج الحاسوب، أو غيرها من أشكال تعتمد على التمثيل الإلكتروني.

البيانات الشخصية: هي كل بيان من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنا بصفة مباشرة، أو غير مباشرة، مثل: الاسم، الرقم الوطني، رقم ورقة العائلة، رقم قيد العائلة، رقم الهاتف، العنوان، رقم الهوية الشخصية، الصور الشخصية، صور المستندات الشخصية، البريد الالكتروني، الإقامة للأجانب وغير ذلك من البيانات ذات الطابع الشخصي.

بيانات الشركات: ويقصد بها الجهات الاعتبارية سواءً عامة أو خاصة مثل: رقم العميل، رقم الحساب، رصيد الحساب، العمليات على الحساب، الرمز الإحصائي، النظام الأساسي، السجل التجاري، الترخيص التجاري، رسالة الإشهار، هيكلة الملكية.

البيانات المالية: رقم العميل، رقم الحساب (محلي او دولي)، رصيد الحساب، العمليات على الحساب، بيانات البطاقة المصرفية (محلية أو دولية)، البيانات الائتمانية، بيانات المحافظ الالكترونية، الحوالات، بيانات الدفع (سواءً الدافع أو المدفوع له أو طريقة الدفع)، أرقام الدفاتر، ويجب التعامل مع أي معلومات شخصية مرتبطة ببيانات الشركات مثل بيانات الإتصال للموظفين أو الملاك وفقا لأحكام حماية البيانات الشخصية.

البيانات الائتمانية: كل بيان شخصي لفرد أو لشخص إعتباري يتعلق بطلب الفرد الحصول على تمويل أو حصوله عليه من جهة تمارس التمويل، بما في ذلك أي بيانات تتعلق بقدرته على الحصول على ائتمان أو بقدرته على الوفاء به وبتاريخه الائتماني.

البيانات: وتشمل البيانات الشخصية، وبيانات الشركات، والبيانات المالية، والبيانات الإئتمانية.

البيانات الحساسة: هي فئة خاصة من البيانات الشخصية تتطلب حماية إضافية نظراً لطبيعتها الحساسة والمخاطر العالية المرتبط بمعالجتها وتشمل على سبيل المثال لا الحصر (البيانات الصحية، البيانات الوراثية، البيانات البيومترية).

صاحب البيانات الشخصية: الفرد الذي تتعلق به البيانات الشخصية.

الولي الشرعي: الشخص الذي يمثل القاصر، أو المحجور عليه لدى المحاكم وينوب عنه في جميع الاعمال القانونية والتصرفات المالية.

الأموال: هي الأصول أو الممتلكات أيًا كان نوعها سواء كانت مادية، أو غير مادية، ملموسة، أو غير ملموسة، منقولة، أو ثابتة أيًا كانت طريقة الحصول عليها، وكافة الحقوق المتعلقة بها، وجميع المستندات أو الوثائق المثبتة لحق ملكيتها أو ملكية حصة فيها أيًا كان شكلها، بما في ذلك المستندات الالكترونية أو الرقمية وتشمل على سبيل المثال لا الحصر:

1. النقود بالعملات المحلية والأجنبية والعملات الافتراضية والالكترونية وأرصدة الحسابات المصرفية.
2. الأوراق التجارية.
3. الاعتمادات المصرفية.
4. الصكوك السياحية.
5. الحوالات المالية والأوراق المالية كالأسهم والسندات والاعتمادات المستندية والمستندات برسم التحصيل وبوالص التأمين.
6. الكمبيالات.

المحفظة الالكترونية: هي حساب يحتوي على قيمة النقود الالكترونية يمتلكه العميل في شركات الدفع الالكتروني.

أنظمة الدفع الالكترونية: هي مجموعة البرمجيات أو الترتيبات أو إجراءات التشغيل ونظم المعلومات وشبكات الاتصال المعدة للدفع أو التحويل أو التقاص أو التسويات للأموال إلكترونيا وبأي عملة كانت، وتنقسم الى:

-أنظمة مدفوعات التجزئة.

-أنظمة الدفع عالية القيمة.

-أنظمة تسوية الأوراق المالية.

-أنظمة التحويل المالي وصرف العملات الأجنبية.

أدوات الدفع: كل أداةٍ تمكن المستخدم من الحصول على الأموال والسلع والخدمات أو القيام بعمليات الدفع وتحويل الأموال.

خدمات الدفع الإلكتروني: هي الخدمات المتعلقة بإدارة النقود الإلكترونية، أي المبالغ التي يتم تداولها إلكترونيا، وكذلك الخدمات المتعلقة بإصداروإدارة أي من أدوات الدفع المدفوعة مسبقاً، أو أي أعمال أخرى تتضمن الحصول على الأموال والسلع والخدمات التي تقرر الجهة المختصة إخضاعها لأحكام هذه التعليمات وذلك بموجب أوامر خاصة تصدرها الجهة المختصة لهذه الغاية.

النقود الإلكترونية: هي قيمة نقدية مستحقة على الطرف الذي قام بإصدارها، وتكون مخزنة إلكترونيا أو مغناطيسيا أو أي وسيلة أخرى، وتصدر مقابل إستلام نقد حقيقي مقابلها يتم إيداعه في حسابات التسوية في المصارف التجارية بغية تنفيذ عمليات الدفع الإلكتروني وتكون وسيلة دفع مقبولة في ليبيا.

البطاقة المالية الإلكترونية: هي وسيط إلكتروني مادي أو افتراضي يستعمل في عمليات السحب أو الإيداع أو الدفع الإلكتروني باستخدام الشبكة المعلوماتية أووسائل تقنية المعلومات.

التشفير: هو عملية تحويل البيانات الإلكترونية إلى رموزغير معروفة أوغير مفهومة يستحيل قراءتها أومعرفتها دون إعادتها إلى هيأتها الأصلية.

النشر: بث أي من البيانات الشخصية عبروسيلة نشر مقروءة أو مسموعة أو مرئية.

المستند القانوني: هو وثيقة توضح حقوق صاحب البيانات ويمكن أن تكون ورقية أو إلكترونية.

قنوات التواصل الرسمية: وهي القنوات التي يتم بها التواصل بين صاحب البيانات وبين المؤسسة المالية، وهي البريد الإلكتروني الموثق، والبوابة الإلكترونية للمؤسسة المالية، والحضور الشخصي لصاحب البيانات لمقر المؤسسة المالية.

المادة الثانية

تحديد البيانات التي تدخل في نطاق نظام حماية البيانات

تسري أحكام هذا النظام على أي بيانات شخصية، أو بيانات شركات، أو بيانات مالية داخل المؤسسة المالية سواءً أكانت عملية جمع، أو معالجة، أو تخزين، أو إزالة لهذه البيانات، وتهدف هذه الاحكام لحماية البيانات الشخصية المجمعة أو المعالجة الكترونياً جزئيا، أوكليا لدى أي مؤسسة مالية.

المادة الثالثة

نطاق تطبيق النظام

يكون نطاق تطبيق النظام في المؤسسات الأتية:

1. مصرف ليبيا المركزي.
2. المصارف الليبية.
3. فروع المصارف الأجنبية وشركات الخدمات المالية العاملة في ليبيا.
4. شركات الدفع الالكتروني.
5. شركات الصر افة المالية.
6. المؤسسات او الشركات التي تمنح الائتمان.
7. شركات التأجير التمويلي.

المادة الر ابعة

تحديد أصحاب البيانات

يقصد بأصحاب البيانات الأشخاص الطبيعيون، أو الشركات، بإعتبارها شخص إعتباري.

المادة الخامسة

تحديد أحقية جمع البيانات

الفقرة (1)

يجب على المؤسسة المالية التي ترغب في جمع البيانات أن تقوم بتوضيح الغرض والسبب من جمع البيانات لأصحاب البيانات. وأن تكون البيانات المطلوب جمعها واضحة لصاحب البيانات.

الفقرة (2)

يجب على المؤسسة المالية التي ترغب في جمع البيانات أن تقوم بتوضيح ما إذا كان جمع البيانات كلها أو بعضها إلزاميًا أم اختياريًا.

الفقرة (3)

يجب على المؤسسة المالية التي ترغب في جمع البيانات إحاطة صاحب البيانات بأن بياناته لن تعالج لاحقاً بصورة تتنافى مع الغرض من جمعها.

الفقرة (4)

يجب على المؤسسة المالية التي ترغب في جمع البيانات أن تقوم أولا بأخذ الموافقة الصريحة مسبقاً من صاحب البيانات ثم تحدد البيانات التي ترغب في جمعها بشكل دقيق وأن تكون البيانات التي يتم جمعها تلبي غرض جمع البيانات بدون زيادة.

الفقرة (5)

لا يجوز أن تكون الموافقة المشار إليها في الفقرة (1) من المادة (الخامسة) من النظام شرطاً لإسداء خدمة، ما لم تكن الخدمة ذات علاقة بجمع البيانات التي صدرت الموافقة عليها.

المادة السادسة

تحديد طرق جمع البيانات

الفقرة (1)

يجب على المؤسسة أن تقوم بجمع البيانات من صاحب البيانات بشكل مباشر، أو من له الولاية الشرعية عليه ومن غير وجود وسيط.

الفقرة (2)

لا يجوز للمؤسسة أن تقوم بجمع البيانات لصالحها عن طريق أي طرف ثالث.

الفقرة (3)

على الجهة أو المؤسسة التي تجمع البيانات التأكد من صحتها وسلامتها أثناء عملية جمعها من صاحبها.

الفقرة (4)

يكون لصاحب البيانات الشخصية الحق في طلب الحصول على بياناته الشخصية المتو افرة لدي المؤسسة المالية بصيغة مقروءة وواضحة وفق الضو ابط والإجراءات التي تحددها اللو ائح .

الفقرة (5)

يكون لصاحب البيانات الشخصية الحق في طلب تصحيح بياناته الشخصية المتو افرة لدى المؤسسة المالية، أو استكمالها، أو تحديثها.

المادة السابعة

تحديد طرق معالجة البيانات

الفقرة (1)

يجب أن تتم أية عملية معالجة على البيانات سواءً أكانت يدوية أو آلية بطريقة تضمن عدم التأثير على البيانات، وعدم تسربها، وكذلك يكون الهدف من عملية المعالجة واضح وتتم المعالجة ضمن الهدف المحدد فقط.

الفقرة (2)

لا يجوز كذلك مُعالجة تلك البيانات إلا لتحقيق الغرض الذي جُمعت من أجله.

الفقرة (3)

لا يجوز للمؤسسة المالية أن تعالج البيانات دون اتخاذ خطوات كافية للتحقق من دقتها، واكتمالها، وحداثتها، وإرتباطها بالغرض الذي جُمعت من أجله وفقاً لأحكام النظام.

المادة الثامنة

تحديد طرق تخزين البيانات

الفقرة (1)

يتم تخزين البيانات داخل مراكز بيانات موجودة داخل حدود الدولة الليبية، ويمنع منعاً باتاً إرسال هذه البيانات خارج الدولة الليبية بأي طريقة كانت.

الفقرة (2)

يتم تطبيق جميع الضوابط الخاصة بتخزين البيانات المذكورة في اللائحة التنظيمية.

المادة التاسعة

تحديد مدة الاحتفاظ بالبيانات

مدة الاحتفاظ بالبيانات هي عشر سنوات كحد أدنى.

المادة العاشرة

تحديد كيفية حماية البيانات

الفقرة (1)

على المؤسسة المالية اتخاذ ما يلزم من إجراءات، ووسائل تنظيمية، وإدارية، وتقنية تضمن المحافظة على البيانات، سواءً عند جمعها، أو تخزينها، أو معالجتها، أو نقلها وفقا للضوابط التي تحددها اللائحة التنظيمية.

الفقرة (2)

تُبلغ المؤسسة المالية الجهة المختصة فور علمها بحدوث تسرّب، أو تلف للبيانات، أو حدوث وصول غير مشروع إليها .

الفقرة (3)

تحدد اللائحة التنظيمية الأحوال التي يجب فيها على المؤسسة المالية إشعار صاحب البيانات في حالة حدوث تسرّب، أو تلف لبياناته، أو حدوث وصول غير مشروع إليها. وإذا كان من شأن حدوث أياً مما سبق أن يرتب ضرراً جسيماً على بياناته، أو على نفسه، فيجب على المؤسسة المالية إبلاغه فوراً.

المادة الحادية عشر

إزالة البيانات

الفقرة (1)

يجب إزالة البيانات في حالة طلب صاحب البيانات ذلك بشكل رسمي عن طريق القنوات الرسمية في حال انتهى الغرض الذي جمعت من أجله.

الفقرة (2)

عند انتهاء مدة الاحتفاظ بالبيانات يجب اتلافها بشكل كامل كما هو منصوص عليه في اللائحة في التنظيمية.

المادة الثانية عشر

البيانات الموجودة لدى المؤسسات المالية

تمنح المؤسسات المالية التي تمتلك البيانات حاليا مدة سنة من تاريخ نشر هذا النظام للامتثال.

المادة الثالثة عشر

مسؤولية الامتثال للنظام

الفقرة (1)

يكون هناك مسمى وظيفي باسم مسؤول البيانات، يتبع لإدارة الامتثال لدى المؤسسة المالية.

الفقرة (2)

يقوم مسؤول البيانات بإرسال التقارير، وتنفيذ الإجراءات اللازمة لتطبيق النظام داخل المؤسسة المالية كما هو موضح في اللائحة التنظيمية.

الفقرة (3)

يكون مسؤول البيانات هو الشخص المسؤول والمحاسب أمام القانون والجهة المختصة فيما يخص تطبيق هذا النظام، وفي حالة حدوث حوادث تنشأ عن عدم تطبيق النظام.

المادة الرابعة عشر

العقوبات

تعاقب كل مؤسسة مالية في حالة عدم امتثالها للنظام بالعقوبات الآتية:

1. غرامة مالية قدرها مئة ألف دينار ليبي، عن كل مخالفة.
2. سحب الترخيص في حالة تكرار المخالفة من المخالف عدا المصارف التجارية.
3. أي عقوبات أخرى ترى الجهة المختصة ضرورة تطبيقها.

المادة الخامسة عشر

الاستثناء التطبيق

يستثني من تطبيق هذا النظام الطلبات التي تصدر عن الجهات القضائية.

المادة السادسة عشر

يعمل بالنظام بعد سنة من تاريخ نشره في الموقع الإلكتروني للجهة المختصة.