MENA FINANCIAL CRIME COMPLIANCE GROUP

Engaging with multi-stakeholders to find solutions to promote leading AML/CTF practices.

دليل عملـــيّ:

إنشاء إطار عمل للخصوصية وحمايــة البيانات

جدول المحتويات

تستند هذه الوثيقة على الممارسات العالمية الرائدة بالإضافة إلى خبرة لجنة العمل التقنيّ في مجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا لتوفير نظرة عامة على المبادئ الأساسية لحماية البيانات والخصوصية. ومع ذلك، فإنها لا تتناول جميع متطلبات الخصوصية ولا تشكّل استشارة قانونيـة.

١.٠ المقدّمـــة

تشكّل الخصوصية وحماية البيانات الشخصية مصدر اهتمام رئيسيّ للعملاء، المؤسسات والجهات الرقابية على حدّ سواء. يتوقّع العملاء من المؤسسات التعامل مع معلوماتهم الشخصية على أنها خاصة وسرّية، حماية بياناتهم الشخصية بشكلٍ فعّال، واستخدامها فقط من أجل توفير وتشغيل الخدمات المالية، ولأغراض أخرى وفقًا لما يقتضي القانون أو النظام. تركز الجهات الرقابية بشكل متزايد على كيفية إدارة المؤسسات للبيانات الشخصية التي بحوزتهم بدءًا من نقطة جمع البيانات وحتى التخلص منها، مع تعزيز حقوق العملاء، بما في ذلك تصحيح بياناتهم الشخصية، الوصول إلى البيانات، والاعتراض على المعالجة عند الاقتضاء. (المرجع: مُلحق (I): تشريعات حماية البيانات في بلدان منطقة الشرق الأوسط وشمال أفريقيا[1]). وفقًا لذلك، أصبحت حماية البيانات الشخصية وثقة العملاء المرتبطة بها ميزة تنافسيّة ومنطقة تركيز حاسمة بالنسبة لمديري المخاطر.

بحكم التعريف، البيانات الشخصية هي أية بيانات تتعلق بفرد محدد أو قابل للتحديد وتُستخدم لتحديد هوية شخص معين. تشتمل الأمثلة على الاسم الكامل، رقم التعريف الشخصي، رقم رخصة القيادة، رقم حساب البنك، رقم جواز السفر، عنوان البريد الإلكتروني، بيانات السكَن، أو واحدة أو أكثر من خصائصهم المادّية، الفيزيولوجية، الفكرية، الثقافية، الاقتصادية، أو الهوية الاجتماعية (المرجع: الملحق (II) – البيانات الشخصية). تسير الخصوصية وحماية البيانات جنبًا إلى جنب. الخصوصية هي حقٌّ إنساني أساسيّ ويتم تعريفها كحقّ أي فرد بالتحكّم بمعلوماته الشخصية الخاصة به بينما حماية البيانات هي عملية حماية المعلومات الخاصة من الفساد، أو الضياع بالإضافة إلى ضمان توفّرها.

الغاية من هذا الدليل، إلى جانب استبيان التقييم الذاتي للخصوصية، هي زيادة الوعي بالامتثال إلى العناصر الرئيسية لبناء إطار عمل فعّال للخصوصية وحماية البيانات حسب الضرورة لتلبية التوقّعات التنظيمية المتطورة والحفاظ على ثقة العملاء.

[1] ستعمل مجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا على تحديث هذا المُلحق حسب الضرورة ليعكس المتطلّبات التنظيمية الجديدة/المنقّحة.

٢.٠ مبادئ الخصوصيّـة وحماية البيـانـات

يجب أن يسعى إطار عمل الخصوصية وحماية البيانات إلى تحقيق المبادئ الرئيسية التالية:

I. **الشرعية، الإنصاف والشفافية –** ينبغي معالجة البيانات الشخصية بإنصاف وشفافية وبالطرق القانونية. لا تتم معالجة البيانات الشخصية لأي فردٍ إلاّ في حال وجود أسباب قانونية لذلك ويجب إعلام الفرد عن كيفية وسبب معالجة بياناته الشخصية إما حين أو قبل جمعها.

II. **تقليل البيانات والحدّ منها –** يجب أن تقتصر البيانات التي تم جمعها على الحد الأدنى من البيانات اللازمة لغرض الجمع فقط. ينبغي أيضًا معالجة البيانات الشخصية للغرض الذي تم جمعها من أجله في البداية فقط. تتطلّب أية معالجة إضافية الحصول على موافقة من العميل ما لم يكن هناك أساس قانوني، مثل تلبية طلب تنظيمي.

III. **الدقّـة –** ينبغي أن تكون البيانات الشخصية دقيقة، وحيث هو مناسب، محدّثة. يجب تصحيح البيانات الخاطئة بأسرع وقت ممكن. تُنصح المؤسسات بتطوير عمليات مستمرة لتحديث البيانات وإتاحة القنوات للعملاء من أجل تحديث بياناتهم. (مثلاً، وجهًا لوجه و عبر الانترنت).

IV. **الاحتفاظ بالبيانات –** لا ينبغي الاحتفاظ بالبيانات لفترة أطول مما هو ضروري للغرض الذي تم جمعها من أجله مع الأخذ بالاعتبار المتطلبات التنظيمية للاحتفاظ بالسجلاّت.

V. **حقوق المعنيين بالبيانات –** يجب أن تقوم المؤسسات بتطبيق العمليات الملائمة لضمان الاستجابة لطلبات المعنيين بالبيانات في الوقت المناسب، حسب الاقتضاء. المعنيون بالبيانات هم الأفراد الذين تخصّهم البيانات الشخصية بما في ذلك العملاء، الموظفون، أعضاء مجلس الإدارة وأطراف ثالثة.

VI. **الأمـن –** يجب حماية البيانات الشخصية من المعالجة غير المسموح بها أو غير القانونية، الضياع بغير قصد، التلف أو إلحاق الضرر، من خلال إجراءات تقنية وتنظيمية مناسبة.

VII. **عمليات نقل البيانات الدولية -** عند نقل البيانات إلى إقليم خارج بلد المؤسسة، يجب أن تكون العناية الواجبة والضوابط فعالة لضمان مستوى كافٍ من الحماية.

VIII. **المساءلـة -** المساءلة هي القدرة على إثبات الامتثال لجميع المبادئ المذكورة أعلاه وهي مطلوبة بموجب اللائحة العامة لحماية البيانات للاتحاد الأوروبي وغيرها من لوائح حماية البيانات في جميع أنحاء العالم. تشمل آليات المساءلة السياسات، والإجراءات، والمبادئ التوجيهية، وقوائم المراجعة وأنشطة التدريب والتوعية، وإجراءات الشفافية، والضمانات التقنية وغيرها من الآليات التي تعمل على تخفيف مخاطر الخصوصية وحماية البيانات الداخلية والخارجية.

تَوضّح الأقسام التالية كيف يمكن ترجمة المبادئ المذكورة أعلاه إلى عمليات فعلية.

٣. ٠ العناصر الرئيسية لإطار فعال للخصوصية وحماية البيانات

الامتثال للخصوصية وحماية البيانات هو بمثابة رحلة تتطلّب الوعي والإدراك المستمرّ لعمليات معالجة البيانات الشخصية وترسيخ إدارة الخصوصية عبر المؤسّسة. اتّباع "نهجٍ واحد يناسب الجميع" ليس هو الجواب أيضًا. ومع ذلك، يمثّل الشكل التالي العناصر الرئيسية المبنيّة على ممارسات عالمية رائدة.

٣.١ الحوكمة والمساءلة

الحوكمة والمساءلة عاملان أساسيّان في بناء إطار عمل متين للخصوصية وحماية البيانات. العناصر الرئيسيّة ملخّصة أدناه:

٣. ١. ١ رؤيـة مجلس الإدارة والاستراتيجية

ينبغي أن تكون حماية البيانات والخصوصية موضوعًا منتظمًا يتم مناقشته على مستوى مجلس الإدارة، نظرًا لنشوء التكنولوجيا عالميًا، زيادة قوانين الخصوصية المتزايدة والوصول العالمي إلى العملاء. بالإضافة إلى ذلك، يجب وضع الخصوصية وحماية البيانات في صميم رؤية المؤسسة. يتم تحقيق ذلك من خلال التزام الإدارة العليا والتدريب والتوعية المستمرّين للموظفين. كجزء من عمله الرقابي، يجب أن يتأكّد المجلس أن الإدارة تتفهم بيئة الخصوصية وتُدرك آثارها على نموذج عمل المؤسّسة. ينبغي تزويد المجلس بالمعلومات الإدارية المفيدة والمناسبة التي تسمح له بممارسة الرقابة الفاعلة. وهذا يتضمّن عدد خروقات البيانات، نتائج خروقات البيانات الوهمية، إحصاءات تدريب الموظفين، ونتائج التدقيق والمراجعة ذات الصلة، وانتهاكات السياسة عالية المخاطر.

٣. ١. ٢ النطـاق الإقليمـي

يتوجّب على المؤسسات مراعاة قوانين الخصوصية التي تنطبق عليها والآثار المترتبة على الامتداد خارج الحدود الإقليمية. تواجه المؤسسات التي لديها مكاتب أو مؤسسات فرعية أو شركات تابعة لها في دول عدة، احتمالية أكبر لأن تؤثر لوائح خصوصية البيانات المختلفة عليها. من أجل بناء خط الأساس، ينبغي على المؤسسات التركيز على مكان حفظ البيانات الشخصية، جمعها، أو معالجتها والتركيز أيضًا على مجالات مشتركة تشمل التسويق، الموارد البشرية، المالية، تكنولوجيا المعلومات/ الأنظمة والتطبيقات. من الممكن أن تساهم معرفة مكان تدفق البيانات، عبر استخدام نشاط تحديد البيانات وطبيعة المعالجة عليها الموضّح في هذه الوثيقة (القسم 5)، في تحديد المتطلبات القابلة للتطبيق.

٣. ١. ٣ المساءلة والأدوار والمسؤوليات

يجب أن تتطلّع المؤسسات إلى بناء وحدات خاصة بحماية البيانات والخصوصية بحيث تكون مسؤولة عن أنشطة حماية البيانات والخصوصية العامـة. عند أخذ القرار بشأن نموذج الخصوصية الملائم، يمكن للمؤسسات الاختيار بين النموذج المركزي، اللامركزي أو الهجين من أجل تطوير استراتيجية الخصوصية الخاصة بها. يستخدم النموذج المركزي وظيفة قناة واحدة بحيث تستدعي أن تقع مسؤولية الخصوصية على عاتق فريق واحد. يفوّض النموذج اللامركزي المسؤوليات الرئيسية إلى المستويات الدنيا من الهيكل التنظيمي. يدمج النموذج الهجين النموذجين المركزي واللامركزي معًا ويُستخدم عادة حيث يكون لدى المؤسسات مكاتب أو كيانات متعددة. العناصر الرئيسية التي يجب مراعاتها عند تحديد نطاق الحجم والبُنية هي:

I. **مسؤول حماية البيانات -** على المؤسسات النظر في تعيين مسؤول حماية البيانات على أن يكون مسؤولاً عن أنشطة الخصوصية وحماية البيانات ويقدّم التقارير إلى أعلى مستوى إداري مباشرة. يجب أن تكون أدوار ومسؤوليات مسؤول حماية البيانات واضحة مع التأكد من عدم وجود تضارب المصالح.

II. **مناصرو الخصوصية وحماية البيانات -** لمزيد من حماية البيانات، يجب على المؤسسات تعيين مناصرين مسؤولين عن الخصوصية وحماية البيانات داخل أقسامهم / إداراتهم. من المتوقّع وجود مُناصر في كل قسم (أي: الموارد البشرية، تكنولوجيا المعلومات، التسويق، الائتمان... الخ).

III. **لجنة حوكمة خصوصية البيانات -** يجب أن تُشكّل لجنة حوكمة ذات اختصاصات مناسبة لمناقشة حوادث الخصوصية، القضايا، والمخاطر. يبيّن تشكيل اللجنة أيضًا اتّجاهًا عامًا في التزام الإدارة العليا بحماية البيانات والخصوصية.

تعيين مسؤول حماية البيانات – الاعتبارات الرئيسية	
ما هي الأدوار الرئيسيّة	▪ تأكيد الالتزام بالمتطلّبات التنظيمية للخصوصية وحماية البيانات. ▪ اعتماد ثقافة الحفاظ على الخصوصية وحماية البيانات وإبلاغ أصحاب المصلحة بسياسات حماية البيانات الشخصية. ▪ الإشراف على عملية الاستجابة لطلبات المعنيين بالبيانات في ممارسة حقوقهم. ▪ إدارة الشكاوى والاستفسارات ذات الصلة بحماية البيانات الشخصية. ▪ تنبيه الإدارة بأي مخاطر قد تنشأ فيما يتعلّق بالبيانات الشخصية التي تتعامل معها المؤسسة. ▪ ضمان الالتزام بالمتطلبات التنظيمية المرتبطة بأي خرقٍ بالاستناد إلى خطة الاستجابة للحوادث. ▪ التواصل مع السُلطات التنظيمية بشأن مسائل حماية البيانات في حال الضرورة.
كيف يجب أن يتم تعيين مسؤول حماية البيانات	من الناحية المثالية، يجب أن يتم تعيين مسؤول حماية البيانات من الإدارة العليا. تقع هذه المسؤولية على عاتق موظف واحد، مجموعة من الموظفين أو من مصدر خارجي. عند الاستعانة بمصادر خارجية لوظيفة مسؤول حماية البيانات، يجب على المؤسسة أن تضمن أن الفرد المعين من قِبل الإدارة العليا يظل مسؤولاً عن العمل مع مسؤول حماية البيانات الخارجي.

٢.٣ سياسات، إجراءات وإشعارات الخصوصية

تُعتبر السياسات والإجراءات ضرورية لربط مبادئ خصوصية البيانات والسماح بالتشغيل السليم للمؤسسة من خلال وضع حدود للسلوك، وضع الخطوط العريضة للعمليات وتحديد القواعد. يجب وضع إجراءات واضحة ومفصلة وإعلانها للأطراف ذات الصلة في جميع أنحاء المؤسسة لضمان الامتثال. من أجل تأسيس إطار عمل متين لحماية البيانات، ينبغي الأخذ بالاعتبار ما يلي:

I. **سياسات وإجراءات –** كحد أدنى، يجب على المؤسسة النظر في إنشاء سياسة حماية البيانات بما في ذلك حقوق المعني بالبيانات المعمول بها وسياسة إدارة الخرق. يجب وضع إجراءات واضحة ومفصلة وإعلانها للأطراف ذات الصلة في جميع أنحاء المؤسسة لضمان الامتثال.

II. **التقييمات والتأكيد –** ينبغي إجراء التقييمات الذاتية وتوثيقها لتقييم ضوابط الخصوصية وحماية البيانات عبر مختلف خطوط الأعمال. (يمكنك الرجوع إلى استبيان تقييم الخصوصية وحماية البيانات لمجموعة الامتثال لمكافحة الجريمة المالية المُتاح على: http://menafccg.com/publications/).

III. **برنامج مراقبة الخصوصية -** يجب إنشاء برنامج مراقبة الخصوصية وتوثيقه لتحديد الثغرات وضمان الفعالية المستمرة. يُعد هذا أمرًا حيويًا لتحديد أي نقاط ضعف قد تظهر بعد التقييم الأولي وكذلك لدفع التحسينات المستمرة في ضوء المخاطر المتطورة مثل المتطلبات التنظيمية المنقّحة وسيناريوهات الخرق.

IV. **بنود حماية البيانات -** يجب أن تضمن المؤسسات أن لديها مجموعة من بنود حماية البيانات لضمان تغطية مخاطر المشاركة أو العملية بشكل كافٍ من خلال البنود المناسبة التي تغطي أي ارتباط مع المعالجين أو مشاركة البيانات مع أطراف ثالثة لغرض إجراء الأعمال الأساسية.

V. **جداول الاحتفاظ بالبيانات -** يجب توثيق معايير الاحتفاظ بالبيانات لضمان الاحتفاظ بجميع البيانات الشخصية طالما كان ذلك ضروريًا فقط، مع مراعاة المتطلبات التنظيمية المعمول بها.

VI. **إشعار الخصوصية -** ينبغي أن يعكس إشعار خصوصية المؤسسة، المنشور على موقعها الإلكتروني بدقّة، كيفية قيام المنظمة بجمع البيانات واستخدامها. يختلف محتوى إشعار الخصوصية من بلدٍ إلى آخر. ومع ذلك، في جميع الحالات، يجب أن يكون إشعار الخصوصية واضحًا وسهل الفهم وألاّ يحتوي على أي مصطلحات معقدة.

إشعار الخصوصية – الاعتبارات الرئيسيّة	
المحتوى	لضمان التوافق مع الممارسات الرائدة، ضع باعتبارك تضمين ما يلي في إشعار الخصوصية الخاص بك: ▪ تفاصيل الاتصال بمسؤول حماية البيانات في مؤسستك. (إن أمكن) ▪ الغايات من المعالجة ▪ المستلمون أو فئات مستلمي البيانات الشخصية. ▪ تفاصيل عمليات نقل البيانات الشخصية إلى أي دولة ثالثة أو منظمات دولية (إن وجدت). ▪ فترات الاحتفاظ بالبيانات الشخصية. ▪ الحقوق المُتاحة للأفراد فيما يتعلّق بالمعالجة. ▪ الحق بسحب الموافقة (إن أمكن) ▪ الحق في تقديم شكوى إلى السلطة الرقابية. (حيث أمكن) ▪ مصدر البيانات الشخصية (إذا لم يتم الحصول عليها من الشخص الذي تتعلّق به). ▪ تفاصيل وجود عملية صنع القرار الآلي، بما في ذلك التنميط (إن أمكن)
المراجعة والتحديث	تذكّر، يجب مراجعة وتحديث إشعار الخصوصية بشكل منتظم. على سبيل المثال، في حال أرادات المؤسسة استخدام البيانات الشخصية لغرضٍ جديد، ينبغي تحديث إشعار الخصوصية وإبلاغ المعنيين بالبيانات.

إشعار الخصوصية – أمثلة عن الممارسة الجيّدة والممارسة السيّئة	
الممارسات الضعيفة: ▪ "قد نستخدم بياناتك الشخصية لتطوير خدمات جديدة". (من غير الواضح ما هي "الخدمات" أو كيف ستساعد البيانات في تطويرها). ▪ "قد نستخدم بياناتك الشخصية لأغراض تتعلّق بالأبحاث". (من غير الواضح ما هو نوع "الأبحاث" المُشار إليها). ▪ "قد نستخدم بياناتك الشخصية لتقديم خدمات ذات طابع شخصي". (من غير الواضح ما يستتبع "إضفاء الطابع الشخصي").	**الممارسات الأفضل:** " قد نستخدم المعلومات المقدمة أو التي تم الحصول عليها عبر هذا الموقع من أجل: الرد على استفساراتك وملاحظاتك (على سبيل المثال، إذا كنت قد طرحت سؤالاً أو أرسلت تعليقات عبر الموقع)، نزودك بالمعلومات أو المنتجات أو الخدمات التي طلبتها، ننفّذ التزاماتنا من أي عقود مبرمة بينك وبيننا، نسمح لك بالمشاركة في أي ميزات تفاعلية للموقع، أو نُبلغك بالتغييرات التي تطرأ على الموقع، أو نزوّدك بالتحديثات حيث وافقت على تلقيها عن طريق التسجيل على هذا الموقع". (من الواضح في هذا المثال نوع المعالجة التي ستجريها المؤسسة)

يتضمن إظهار المساءلة وإرساخ الخصوصية وحماية البيانات عبر المؤسسة مجموعة واسعة من السياسات والإجراءات. ومع ذلك يمكن أن يختلف دور مسؤول الخصوصية وحماية البيانات. الأمثلة تتبع:

دور مسؤول الخصوصية وحماية البيانات – أمثلة	
أمور يتم تطويرها من قبل مسؤول الخصوصية بعد جمع المعلومات من أصحاب المصلحة الرئيسيين	▪ سياسة الخصوصية وحماية البيانات ▪ إشعار الخصوصية ▪ منهج التدريب ▪ إرشادات تقييم تأثير حماية البيانات والخصوصية ▪ سياسة/ إجراء للاستخدامات الثانوية للبيانات الشخصية
أمور يبدي الرأي فيها مسؤول الخصوصية ولكن تم إنشاؤها من قبل أصحاب المصلحة الآخرين	▪ إجراءات التسويق المباشر ▪ سياسات التوظيف ▪ جداول الاحتفاظ بالسجلّات
متاح لمسؤول الخصوصية فور إنجازه لغرض الاحتفاظ بالسجلات والتحقّق من صحّتها	▪ نتائج التدقيق الداخلي ▪ نتائج تقييم أمن تكنولوجيا المعلومات ▪ خطط استمرارية الأعمال

٣.٣ تحديد البيانات والمعالجة التي تتم عليها وتقييمات تأثير الخصوصية

يصف هذا القسم بعض الأدوات التي يمكن استخدامها لإثبات مبادئ خصوصية البيانات ولضمان مراعاة الأنشطة اليومية لحماية البيانات والخصوصية.

٣. ٣. ١ تحديد البيانات والمعالجة التي تتم عليها/ سجلات أنشطة المعالجة

يُعدّ تحديد البيانات، أي الاحتفاظ بسجل لأنشطة معالجة البيانات، مطلبًا للعديد من المؤسسات بموجب القانون العام لحماية البيانات (GDPR) وأفضل ممارسة حتى بالنسبة لتلك التي لا يُطلب منها تطبيقها.

بالإضافة إلى ذلك، قد تطلب السلطات الإشرافية سجلات لأنشطة المعالجة داخل المؤسسة، وإنتاج خريطة البيانات هو جزء واحد من المعلومات التي يمكن أن تساعد في تلبية طلباتهم. بمجرد تجميع قائمة أنشطة المعالجة، يصبح من السهل على المؤسسات تبرير معالجتها أو تحديد المكان الذي يجب الحصول فيه على الأساس القانوني. يُعتبر هذا التطبيق دليلاً على أن المؤسسة تأخذ الخصوصية بعين الاعتبار منذ بدء التصميم وفي جميع أعمالها. في الجوهر، إن المؤسسة التي تنشئ خريطة تدفق بيانات لتقنية أو عملية جديدة تكون مستعدة بشكل أفضل لتطبيق وسائل حماية الخصوصية في مرحلة مبكرة من العملية.

فوائد تحديد البيانات:

I. **إشعارات الخصوصية** - استنادًا إلى تحديد البيانات، يمكن للمؤسسة تقديم إشعارات خصوصية أكثر دقة توضّح أنواع المعالجة التي تجريها على البيانات الشخصية التي بحوزتها.
II. **الأمن** - إن فهم مكان وجود البيانات الشخصية وتدفقها في جميع أنحاء العمل هو الخطوة الأولى لفهم المخاطر التي تسمح بوضع ضمانات وضوابط أمنية مناسبة.
III. **طلبات المعنيين بالبيانات** - كجزء من حقوق المعنيين بالبيانات، قد يسأل العملاء عن البيانات التي تجمعها مؤسستك وإلى أين يتم إرسالها. وجود سجل لأنشطة المعالجة يجعل من السهل الاستجابة في الوقت المناسب.
IV. **الاستجابة لخرق البيانات** - يساعد وجود سجل بيانات مركزي في الاستجابة بشكل أكثر ملاءمة للخرق ومعرفة البيانات التي قد تكون تعرضت للكشف بناءً على المناطق التي تأثرت بالخرق.

٣. ٣. ٢ تقييمات تأثير الخصوصية

تقييم تأثير الخصوصية (Privacy Impact Assessment) هو أداة عملية للمساعدة في تحديد ومعالجة مخاطر حماية البيانات والخصوصية في مرحلة التصميم والتطوير لمشروع ما أو تغيير في العمل. هذا التقييم مصمم لمساعدتك على تحليل مخاطر الخصوصية وتحديدها وتقليلها على الأفراد كلما تم إدخال نظام أو منتج جديد أو خدمة أو عملية تجارية جديدة أو حيث يتم اقتراح تغييرات على العمليات والأنظمة الحالية.

يساعد تقييم تأثير الخصوصية أيضًا المؤسسات على تلبية توقعات الأفراد بشأن الخصوصية وحماية البيانات. كما يساعد على تجنب الإضرار بالسمعة الذي قد يحدث بخلاف ذلك. يمكن أن تكون هناك أيضًا مزايا مالية؛ إذ إن تحديد معضلة أو مشكلة محتملة في وقت مبكر يعني حلًا أبسط وأقل تكلفة بشكل عام.

ومع ذلك، لا يتعين على تقييم تأثير الخصوصية القضاء على جميع المخاطر، ولكن يجب أن يساهم في تقليل وتحديد ما إذا كان مستوى مخاطر الخصوصية وحماية البيانات مقبولًا أم لا في ظل الظروف، مع مراعاة فوائد العملية الجديدة / المنقحة، والمنتج، والخدمة الخ...المَنوي تحقيقها.

٣. ٤ أمن البيانات - التدابير التقنيّـة والتنظيمية

يجب أن تضمن المؤسسة تطبيق التدابير التقنية والتنظيمية المناسبة لحماية البيانات الشخصية بما في ذلك الحماية من المعالجة غير المصرّح بها أو غير القانونية أو الفقدان العرضي أو التدمير أو التلف. تشمل بعض الأمثلة على الإجراءات الأمنية الواجب تنفيذها ما يلي:

I. **إدارة الوصول -** وجود ضوابط مناسبة لإدارة الوصول يحد من الوصول إلى البيانات الشخصية للموظفين المصرح لهم بذلك فقط. يضمن الفصل بين الواجبات ومبادئ الامتيازات أن يكون لدى المستخدمين إجراءات وفقًا لأدوارهم فقط.

II. **الهوية المستعارة والتشفير -** تحديد الهوية المستعارة (Pseudonymization) هو معالجة البيانات الشخصية بحيث لا يمكن أن تُعزى البيانات إلى صاحب بيانات معيّن دون استخدام معلومات إضافية. يستلزم التشفير استخدام خوارزمية لخلط البيانات أو تشفيرها ثم استخدام مفتاح لكي يتسنّى للطرف المتلقّي فك تشفير المعلومات أو حل رموزها.

III. **إدارة الاستجابة لحادث -** تعالج إدارة الاستجابة لحادث المتطورة مراحل الحادث بما في ذلك الإعداد والتعرف والاحتواء والتعافي والدروس المستفادة. تتطلب قوانين حماية البيانات إخطار السلطات وأصحاب البيانات المتأثرة في ظل ظروف وأطر زمنية معينة. على سبيل المثال تُلزمُ اللائحة العامة لحماية البيانات (GDPR) المؤسسات بإبلاغ السُلطات في غضون 72 ساعة بعد المعرفة بحدوث خرق. تحدد العملية المُحكمة للاستجابة للحوادث خروقات البيانات المحتملة في الوقت المناسب.

IV. **إدارة مخاطر الأطراف الثالثة –** تمكّن إدارة مخاطر الأطراف الثالثة المؤسسات من تحديد الضوابط الرئيسية بشكل مناسب والتي يجب تنفيذها من قِبل معالجي البيانات لتقليل مخاطر الخصوصية.

V. **منع تسرّب البيانات -** يتم تعريف منع تسرب البيانات على أنها ممارسة للكشف عن البيانات غير المصرح بها ومنعها. تُلزمُ بعض المتطلبات التنظيمية في منطقة الشرق الأوسط وشمال إفريقيا على البنوك فرض تدابير لمواجهة مخاطر التنزيل غير المصرح به لبيانات العملاء وفقدان البيانات التي تحتوي على معلومات حساسة من خلال تنفيذ حلول لمنع تسرّب البيانات. يساعد حل منع تسرّب البيانات الفعال المؤسسات على فهم أنواع البيانات الواجب حمايتها، ومراقبة رحلة البيانات بما في ذلك قنوات تسرب البيانات وأخيرًا منع تسرب البيانات؛ مثل حظر أنواع معينة من الرسائل / الملفات من مغادرة نطاق المؤسسة. يمكن أن تخفف حلول منع تسرّب البيانات من النوايا الخبيثة والإهمال بالإضافة إلى الكشف غير المقصود عن البيانات.

٣. ٥ حقوق المعني بالبيانات

أحد العناصر الأساسية للخصوصية وحماية البيانات هو حقوق صاحب البيانات. نفذّت البلدان مقاربات مختلفة فيما يتعلق بحقوق المعني بالبيانات، بما في ذلك النطاق والأطر الزمنية التي يجب خلالها الوفاء بهذه الحقوق من قبل المؤسسة. فيما يلي أمثلة على الحقوق الأساسية:

I. **الحق بالحصول على معلومات** - يوفر هذا الحق لصاحب البيانات القدرة على الطلب من المؤسسة الحصول على معلومات حول البيانات الشخصية المتعلقة به/بها والتي تتم معالجتها والأساس المنطقي لهذه المعالجة.

II. **الحق بالوصول إلى البيانات**- يسمح هذا الحق للشخص المعني بالاطلاع على بياناته الشخصية أو النظر إليها، بالإضافة إلى طلب نسخ من البيانات الشخصية.

III. **الحق بطلب التعديل** - يوفر هذا الحق لصاحب البيانات القدرة على طلب تعديلات على بياناته الشخصية في حال اعتقاد صاحب البيانات أن البيانات الشخصية ليست محدثة أو دقيقة.

IV. **الحق في سحب الموافقة** - يجب أن يكون لأصحاب البيانات القدرة على سحب الموافقة الممنوحة مسبقًا لمعالجة بياناتهم الشخصية.

V. **الحق في الاعتراض على القرارات التي تُتخذ على أساس آلي فقط** - اتخاذ القرار الآلي هو أي شكل من أشكال المعالجة الآلية للبيانات الشخصية (بما في ذلك التنميط) الذي ينتج عنه تأثير قانوني أو يؤثر بشكل كبير على صاحب البيانات. يوفر هذا الحق لصاحب البيانات القدرة على الاعتراض على قرار يعتمد على المعالجة الآلية. باستخدام هذا الحق، يمكن للفرد أن يطلب مراجعة طلبه يدويًا، لأنه يعتقد مثلا أن معالجة قرضه قد لا تأخذ بالاعتبار وضعه/ها الاستثنائي.

VI. **الحق في النسيان / الحذف** - يمنح هذا الحق صاحب البيانات القدرة على طلب حذف بياناته. سينطبق هذا بشكل عام على الحالات التي تنتهي فيها العلاقة مع العميل. من المهم ملاحظة أن هذا الحق ليس حقًا مطلقًا، ويعتمد على الجدول الزمني للاحتفاظ لدى المؤسسة بما يتماشى مع القوانين الأخرى المعمول بها.

VII. **الحق في نقل البيانات** - يوفر هذا الحق لصاحب البيانات القدرة على طلب نقل بياناته/ها الشخصية. كجزء من هذا الطلب، قد يطلب صاحب البيانات إعادة بياناته/ها الشخصية إليه/ها أو نقلها إلى مؤسسة أخرى.

اعتبارات بشأن تطوير سياسة التعامل مع طلبات أصحاب البيانات لممارسة حقوقهم

عند وضع سياسة داخلية للتعامل مع طلبات أصحاب البيانات، يجب على المؤسسات مراعاة ما يلي:

- كيف تنوي المؤسسة استقبال جميع الطلبات، أي القنوات الخاصة بتقديم الطلبات.
- ما هي المعلومات المطلوبة من صاحب البيانات.
- حيثما يسمح القانون المحلي بذلك، كيف تحسب المؤسسة الرسوم بطريقة تعكس بدقة الوقت والجهد اللازمين للاستجابة للطلب.
- كيف تضمن المؤسسة معالجة الطلبات في غضون الإطار الزمني التنظيمي وما هو الردّ الذي سيقدّم للفرد في حال عدم قدرة المؤسسة على تلبية الطلب خلال هذا الإطار الزمني.
- ما هي الإجراءات التي وضعتها المؤسسة للتحقق من هوية الفرد مقدّم الطلب.
- ما هي عملية التوثيق التي تقوم بها المؤسسة لتسجيل الطلبات الواردة والمعالَجة. قد تتضمن الوثائق أيضًا الطلبات التي تم استلامها ولكن لم تتم معالجتها بسبب استثناء قابل للتطبيق.
- ما هي سياسة الاحتفاظ في المؤسسة التي تحكم حفظ سجلات الطلبات الواردة.

الحق في الاعتراض على القرارات التي تُتخذ على أساس آلي – قضايا تؤخذ بالاعتبار

"فقط"	**"فقط"** تعني عملية صنع القرار بشكل آلي بالكامل وتستبعد أي تأثير بشري على النتيجة. لا يزال من الممكن اعتبار العملية آلية فقط إذا قام إنسان بإدخال البيانات المراد معالجتها، ومن ثم تم اتخاذ القرار بواسطة نظام آلي. لن يتم اعتبار العملية آلية فقط إذا فسّر شخص ما نتيجة القرار الآلي قبل تطبيقه على الفرد. ▪ <u>مثال:</u> يتم إصدار تحذير للموظف بسبب التأخر في الحضور إلى العمل. تم إصدار التحذير لأن نظام تسجيل الدخول الآلي للمؤسسة أشار إلى حقيقة أن الموظف قد تأخر في عدد محدد من المناسبات. ومع ذلك، على الرغم من إصدار التحذير على أساس البيانات التي تم جمعها بواسطة النظام الآلي، فقد اتُخذ قرار إصداره من قبل مدير الموارد البشرية لدى صاحب العمل بعد مراجعة تلك البيانات. في هذا المثال، لم يتم اتخاذ القرار فقط بالطريقة الآلية. **تذكر: السؤال هو ما إذا كان إنسان يقوم بمراجعة القرار قبل تطبيقه ولديه حرّية التصرّف لتغييره، <u>أو</u> ما إذا كان يقوم ببساطة بتطبيق القرار الذي اتخذه النظام الآلي.**
" هام "	القرار الذي ينتج عنه تأثير كبير هو أمرٌ يؤثر على الوضع القانوني للشخص أو حقوقه القانونية. في الحالات القصوى، قد يستبعد الأفراد أو يميّز بينهم. القرارات التي قد يكون لها تأثير ضئيل بشكل عام، قد تؤثر بشكلٍ كبير على الأفراد الأكثر ضعفًا، مثل الأطفال. ▪ <u>أمثلة:</u> ▪ الرفض التلقائي لطلب الائتمان عبر الإنترنت. ▪ ممارسات التوظيف الإلكتروني دون تدخل بشري. ▪ يتقدم الفرد بطلب للحصول على قرض عبر الإنترنت. يستخدم موقع الويب الخوارزميات وبحث الائتمان الآلي لتقديم قرار فوري بنعم / لا بشأن الطلب.

٣. ٦ معالجــو البيانــات

يضطلع المراقب (أي مدير البيانات) أو معالج البيانات الشخصية بأدوار ومسؤوليات مختلفة، وبالتالي من المهم بالنسبة للمؤسسات معرفة الدور الذي تلعبه. بموجب القانون العام لحماية البيانات وقوانين الخصوصية وحماية البيانات الأخرى، يتحمل مراقب البيانات مسؤوليات أكبر فيما يتعلق بحماية خصوصية وحقوق الأشخاص المعنيين بالبيانات.

يحدد المراقبون أهداف ووسائل معالجة البيانات الشخصية. في الجوهر، هم الذين يصنعون قرارات بشأن أنشطة المعالجة، بينما المعالجون هم أطراف ثالثة تعالج البيانات بناءً على تعليمات المراقب.

عندما يعيّن المراقب معالجًا، يجب عليه إجراء العناية الواجبة الكافية وإدراج بنود حماية البيانات المناسبة لتحديد الدور والأغراض التي تحدّد بوضوح متى يُمكن للمعالج معالجة البيانات الشخصية. بموجب اللائحة العامة لحماية البيانات GDPR وبعض قوانين الخصوصية، يجب على المراقب إجراء تقييمات تأثير الخصوصية عندما يوجّه المعالجين لتنفيذ أنشطة معالجة بيانات عالية الخطورة. أخيرًا، في حالة حدوث خرق للبيانات، يجب على المراقبين إخطار السلطات الإشرافية وأصحاب البيانات كلما أدى الانتهاك إلى تعريض حقوق وحريات أصحاب البيانات للخطر. من ناحية أخرى، يجب على المعالج إخطار المراقب ذي الصلة المتأثر بالخرق.

العقود المُبرمـة مع معالجي البيانات – الاعتبارات الرئيسيّة

ضع في اعتبارك تضمين ما يلي في العقود المُبرمة بينك وبين معالجي البيانات:

- ✓ يجب أن يتصرف المعالج فقط بناءً على التعليمات المكتوبة للمراقب (ما لم يكن مطلوبًا بموجب القانون التصرف بدون هذه التعليمات)،
- ✓ يجب على المعالج التأكد من أن أي فرد يقوم بمعالجة البيانات يخضع لواجب الثقة،
- ✓ يجب أن يتخذ المعالج الإجراءات المناسبة لضمان أمن المعالجة،
- ✓ للمعالج إشراك معالج فرعي فقط بموافقة مسبقة من مراقب البيانات وبموجب عقد خطّي،
- ✓ يجب على المعالج مساعدة مراقب البيانات في السماح لأصحاب البيانات بممارسة حقوقهم حسب الاقتضاء،
- ✓ يجب على المعالج مساعدة مراقب البيانات في الوفاء بالالتزامات التنظيمية فيما يتعلق بأمن المعالجة، والإخطار بانتهاكات البيانات الشخصية وتقييمات تأثير حماية البيانات،
- ✓ يجب على المعالج حذف أو إعادة جميع البيانات الشخصية إلى المراقب كما هو مطلوب في نهاية العقد، و
- ✓ يجب أن يخضع المعالج لعمليات التدقيق والتفتيش من قِبل مراقب البيانات.

المراقب والمعالج – الفرق الرئيسي

تذكّر: يُحدد المراقب الغرض من معالجة البيانات، أي "لماذا" يتم استخدام البيانات والوسائل، أي "كيفية" معالجة البيانات. من ناحية أخرى، يلتزم المعالج بالتعليمات المقدمة من المراقب ويعمل فقط "نيابة عن" المراقب أثناء معالجة بيانات المراقب.

٣. ٧ نقل البيانات ومشاركة البيانات

كقاعدة عامة، يُسمح بعمليات النقل عبر الحدود عند نقل البيانات إلى دولة تتمتّع بقوانين مناسبة لحماية البيانات . يجب على المؤسسات مراجعة خرائط تدفق البيانات الخاصة بهم لمعرفة مكان حدوث عمليات النقل عبر الحدود. عند اكتمال التقييم، يجب على المؤسسات مراجعة ما إذا كانت هذه الدول لديها تشريعات ملائمة لحماية البيانات. إذا لم يكن الأمر كذلك، فيجب عليهم التأكد من إجراء العناية الواجبة الكافية بالإضافة إلى تضمين الضمانات المناسبة والبنود التعاقدية في الاتفاقيات.

٣. ٨ التدريب والتوعيـة

تمكّن ثقافة الخصوصية وحماية البيانات المتينة الموظفين في المؤسسة من المساهمة في تحقيق هدف مشترك بثقة وتصميم. يجب أن يكون جميع الموظفين على دراية بأدوارهم ومسؤولياتهم في حماية البيانات الشخصية. هناك العديد من الطرق لتعزيز وتحسين ثقافة الخصوصية باستمرار، وهي تشمل:

I. **التدريب والتوعية** - كحد أدنى، يجب أن يتلقى جميع الموظفين تدريبًا سنويًا على خصوصية البيانات. قد يحتاج بعض الموظفين المعرّضين بشكلٍ أكبر للبيانات الشخصية إلى تدريب إضافي أو متخصص. يوصى بالنشرات الداخلية وورش العمل والكتيّبات كوسائل متواصلة لزيادة الوعي وفرض الالتزام بحماية البيانات الشخصية.

II. **الرسائل الإخبارية** - بشكل منتظم، يوصى بتضمين محتوى حماية البيانات كجزء من الرسائل الإخبارية الموجودة أو القائمة بذاتها. يجب أن تكون النشرة الإخبارية غنيّة بالمعلومات المتعلّقة بأخبار الخصوصية الحالية والغرامات المفروضة على الجهات المخالفة والدروس المستفادة.

III. **إجراءات التوظيف** - يجب أن يكون الموظفون (الموظفون بدوام كامل / جزئي والمتعاقدون وموظفو الأطراف الثالثة) على دراية بأدوارهم ومسؤولياتهم تجاه حماية البيانات الشخصية لدى المؤسسة، ويجب أن يكونوا على دراية بالتهديدات الرئيسية لهذه الأصول. ينبغي معالجة مسؤوليات الخصوصية قبل التوظيف عبر توصيفات وظيفية مناسبة وضمن شروط وأحكام التوظيف.

تذكّر أن التدريب، التوعية وبناء القدرات هم بمثابة رحلة. يتعيّن على المؤسسة أن تضمن أن تدريبها وتوعيتها يتعاملان مع جميع المستويات والالتزام بالخصوصية وحماية البيانات التي تتوالى من أعلى إلى أسفل عبر المؤسسة.

التدريب والتوعية – اعتبارات رئيسية		
الهدف	التوقيت	التفاصيل
مجلس الإدارة	• في بداية رحلة حماية البيانات الشخصية للمؤسسة. • بشكل دوري لضمان مواكبة مجلس الإدارة للتطورات التنظيمية وأفضل الممارسات والمخاطر المتطورة	وعي مجلس الإدارة بمخاطر حماية البيانات الشخصية وإدراج مخاطر حماية البيانات الشخصية في إطار عمل إدارة مخاطر المؤسسة
الإدارة العُليا	• في بداية رحلة حماية البيانات الشخصية للمؤسسة. • بشكل دوري (على سبيل المثال أثناء صياغة تقرير التدقيق السنوي الداخلي)	ترشيد الفوائد التجارية لحماية البيانات الشخصية، وتسليط الضوء على الأدوار الرئيسية للإدارة العليا، وإنشاء بنية الإبلاغ عن المخاطر لتحديد وإدارة المخاطر
جميع الموظفين	• عند التوظيف (على سبيل المثال خلال 3 أشهر من التوظيف) • على أساس دوري (على سبيل المثال سنويًا) • مخصص عند إجراء مراجعة لقوانين حماية البيانات أو سياسات وعمليات حماية البيانات الخاصة بالمؤسسة	تثقيف الموظفين بشأن المتطلبات التنظيمية وسياسات وعمليات حماية البيانات في المؤسسة. تذكر أنه من المهم توفير مواد التدريب على حماية البيانات ضمن منصّة أساسية يمكن الوصول إليها (مثل الإنترنت).
الموظفون الذين يتعاملون مع البيانات الشخصية	• عند التعيين في دور وظيفي محدّد أو تغيير في نطاق الدور / الوظيفة. • عندما تكون هناك سياسات أو عمليات جديدة لحماية البيانات	تدريب متعمق على حماية البيانات خاص بالسياسات والعمليات الداخلية
شهادات احتراف	• كجزء من التطوير الوظيفي	مسؤول حماية البيانات والموظفون الذين يشكلون جزءًا من فريق مسؤول حماية البيانات

٣. ٩ إدارة الخرق

خرق البيانات الشخصية يعني خرقًا للأمن يؤدّي إلى التدمير العرضي أو غير القانوني أو فقدان أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية. وهذا يشمل الخروقات الناتجة عن أسباب عرضية ومتعمدة على حدّ سواء. يمكن أن تحدث خروقات البيانات الشخصية لأسباب مختلفة مثل النشاط الضار أو الخطأ البشري أو خطأ في نظام الكمبيوتر.

يتوجب على المؤسسات تطوير وتنفيذ عملية إدارة خرق البيانات الشخصية لمعالجة حوادث الاختراق. ينبغي أن تتضمن الخطة الإجراءات المناسبة التي تحكم جميع الأنشطة الرئيسية التالية ؛ احتواء الخرق تقييم المخاطر، الإبلاغ عن الحادث، تقدير الاستجابة، والتعافي لمنع الانتهاكات المستقبلية.

إدارة الخرق – الخطوات الرئيسيّة لإدارة فعّالة	
الاحتواء:	▪ تأكّد من خطورة الانتهاك، وما إذا كان يتضمن أية بيانات شخصية وما إذا كان الخرق لا يزال يحدث. ▪ في حال استمرار حدوث الخرق، حدّد الخطوات التي يجب اتخاذها على الفور لتقليل تأثير الخرق واحتوائه كي لا يتمّ فقدان المزيد من البيانات (على سبيل المثال تقييد الوصول إلى الأنظمة أو إغلاق النظام وما إلى ذلك). ▪ نفّذ الخطوات المناسبة المطلوبة لاسترداد أي فقدان للبيانات حيثما أمكن والحد من الضرر الناجم (مثل استخدام النسخ الاحتياطية لاستعادة البيانات وتغيير كلمات المرور وما إلى ذلك). ▪ أبلِغ لجنة الامتثال التابعة لمجلس الإدارة / لجنة المخاطر التابعة لمجلس الإدارة إذا كانت خطورة الانتهاك وتأثيره المحتمل يستدعي ذلك. ▪ اطلب المشورة القانونية أو مشورة الخبراء في حال الظن بحدوث نشاط غير قانوني أو من المحتمل حدوثه. ▪ تأكّد من إعداد التقارير التنظيمية لتبليغ الجهات الرقابية ضمن الأطر الزمنية المحددة. ▪ تأكد من أن الإجراءات والقرارات موثقة بالكامل وتم تسجيلها في سجل خرق أمان البيانات.
تقييم المخاطر:	لمساعدة المؤسسة في تحديد مسار العمل التالي، يتم إجراء تقييم للمخاطر المرتبطة بالخرق لتحديد ما إذا كان من المحتمل حدوث أي عواقب سلبية محتملة على الأفراد وخطورة هذه العواقب. القضايا الرئيسية للأخذ بالاعتبار: ▪ ما هي أنواع وحجم البيانات المعنية؟ ▪ هل هناك بيانات حساسة تأثرت بالخرق؟ ▪ هل تم الكشف عن البيانات أو فقدانها أو سرقتها بشكل غير رسمي؟ هل تم وضع وسائل لمنع الوصول / سوء الاستخدام؟ (مثل التشفير) ▪ كم عدد الأفراد المتأثرين بخرق المعلومات؟ ▪ ماذا يمكن أن تُفصح البيانات للطرف الثالث عن الفرد؟ هل يمكن إساءة استخدامها بغض النظر عمّا حدث للبيانات؟ ▪ ما هو الضرر الفعلي/المحتمل الذي قد يحدث لهؤلاء الأفراد؟ مثلاً، السلامة

	الجسدية، السمعة، الأوضاع المالية، سرقة الهوية، والجوانب الخاصة الأخرى في حياتهم. ▪ هل هناك عواقب أكبر ليتم النظر فيها؟
التقديـــر والاستجابـــة:	عندما تؤدّي استجابة المؤسسة لخرق البيانات إلى نتيجة، يجب على المؤسسة: ▪ القيام بمراجعة كاملة لأسباب الخرق وفعالية الاستجابة على حد سواء. ▪ يجب إبلاغ لجنة الخصوصية وحماية البيانات بالمراجعة الكاملة لتزويدها بالمعلومات والمناقشة في أقرب وقت ممكن بعد تحديد خرق البيانات. ▪ إذا تم من خلال المراجعة تحديد المشكلات المنهجية أو المستمرة المرتبطة بنقاط الضعف في العمليات الداخلية أو الإجراءات الأمنية كسبب لخرق البيانات، يجب حينذاك صياغة خطط عمل مناسبة واتخاذ إجراءات بشأنها ومراقبتها لتصحيح أي مشكلات وتنفيذ التوصيات الخاصة بالتحسينات. ▪ يجب على اللجنة رصد التقدم المُحرز مقابل الإجراءات بشكل مناسب.

٣. ١٠ المراقبة المستمرّة والتحقّق

- **عمليات التدقيق المستقلّـة:** تعزّز عمليات التدقيق المستقلة ثقافة الخصوصية من خلال التحسين المستمر للعمليات والضوابط الداخلية وضمان المساءلة. يجب أن تتضمن عملية تدقيق المؤسسة أيضًا تمرينًا على اختراق البيانات أو التحقيق. قد تنظر المؤسسة أيضًا في إشراك طرف ثالث لإجراء عمليات تدقيق / تقييمات.
- **مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية:** تكفلُ مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية، المتعلقة بإطار وأنشطة حماية البيانات، أن تكون ثقافة الخصوصية قابلة للتنفيذ والقياس. وتشمل هذه على سبيل المثال لا الحصر عدد انتهاكات البيانات، و تقييمات تأثير الخصوصية المكتملة، ومشكلات الخصوصية التي تصاعدت من قبل مناصري الخصوصية، معدلات إتمام التدريب على الخصوصية وحماية البيانات، ونتائج تمارين الخرق الوهمي.
- **المقارنة مع أفضل الممارسات:** يجب على المؤسسة أيضًا مواكبة تطورات أفضل الممارسات من أجل تحديد مجالات التعزيز ودفع التغييرات اللازمة للاستمرار في إضافة قيمة ولِضمان فعالية البرنامج. يجب إضفاء الطابع الرسمي على هذا الأمر من خلال الوصف الوظيفي لمسؤول حماية البيانات.
- **الاحتفاظ بالسجلات:** يجب على المؤسسة توثيق نتائج المراقبة والمراجعات، حسب الضرورة، لإثبات الامتثال للهيئات التنظيمية.

ملحقـــات

I. تشريعات حماية البيانات في بلدان منطقة الشرق الأوسط وشمال أفريقيا

II. البيانات الشخصية (العميل والموظف)

III. استبيان تقييم الخصوصية وحماية البيانات لمجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا

المُلحق (ا): تشريعات حماية الخصوصية في بلدان منطقة الشرق الأوسط وشمال أفريقيا

الجزائــر

تشريع حماية البيانات

تخضع حماية البيانات في الجزائر للقانون رقم 18-07 المؤرخ 10 يونيو 2018 بشأن حماية الأفراد في معالجة البيانات الشخصية ("القانون 18-07") الذي نُشر في الجريدة الرسمية في يوليو 2018.

التعريفات الرئيسية

- تعريف البيانات الشخصية: أي معلومات، بغض النظر عن طبيعتها، تتعلق بشخص تم تحديده أو تحديد هويته، بطريقة مباشرة أو غير مباشرة، ولا سيما بالرجوع إلى رقم التعريف أو إلى عنصر واحد أو أكثر من عناصره المادية والفسيولوجية والجينية والبيو مترية والنفسية والاقتصادية أو الهوية الثقافية أو الاجتماعية.
- تعريف البيانات الشخصية الحسّاسة: يتم تعريف البيانات الشخصية الحساسة بموجب القانون على أنها بيانات شخصية تكشف عن الأصل العرقي أو العنصري، الآراء السياسية، المعتقدات الدينية أو الفلسفية، أو العضوية النقابية للشخص المعني أو المتعلقة بصحته، بما في ذلك بياناته الوراثية.

السلطــة

ينشئ القانون 18-07، بالاشتراك مع رئيس الجمهورية، سلطة إدارية مستقلة لحماية البيانات الشخصية. هذه السلطة الوطنية مسؤولة عن ضمان معالجة البيانات الشخصية وفقًا للقانون 18-07.

مسؤولو حماية البيانــات

لا يتطلب تعيين مسؤول حماية البيانات بموجب القانون 18-07.

التسجيل

يجب تسجيل مراقب البيانات الشخصية في سجل حماية البيانات الوطني الذي تحتفظ به السلطة الوطنية. بالإضافة إلى ذلك، تخضع أي عملية معالجة للبيانات الشخصية لإعلان أو إذن مسبق من قِبل السلطة الوطنية.

معالجة البيانــات

لا يجوز معالجة البيانات الشخصية إلا بموافقة صريحة من الشخص المعني. هذه الموافقة المسبقة ليست مطلوبة في بعض الحالات المدرجة بشكل حصري في القانون 18-07. على سبيل المثال، عند:

- الامتثال لالتزام قانوني ينطبق على الشخص المعني أو مراقب البيانات الشخصية.
- تنفيذ عقد يكون الشخص المعني طرفاً فيه أو تنفيذ التدابير التعاقدية المسبقة المتخذة بناءً على طلب الشخص المعني.
- تحقيق مصلحة مشروعة لمراقب البيانات أو متلقي البيانات.

حقوق صاحب البيانــات

- الحق في الحصول على معلومات مسبقة - حق الوصول - حق التصحيح - حق الاعتراض

نقل البيانات

- تسمح السلطة بنقل البيانات الشخصية عبر الحدود خارج الجزائر، بعد التأكد من أن البلد المتلقي لديه تدابير خصوصية بيانات كافية.
- يمكن لمراقبي البيانات نقل البيانات عبر الحدود إلى بلد ما دون تدابير حماية البيانات الكافية في حالات معينة. على سبيل المثال:
  - إذا قدم صاحب البيانات موافقته الصريحة على النقل.
  - لتنفيذ عقد بين صاحب البيانات ومراقب البيانات، أو الإجراءات التعاقدية المسبقة بناءً على طلب صاحب البيانات.
  - بناءً على الحصول على ترخيص من السلطة بالنقل.

إشعار الخرق

لا يوجد أي التزام بالإبلاغ عن الخرق من قبل مراقب البيانات إلى الجهة الرقابية أو أصحاب البيانات.

البحريـن

تشريع حماية البيانات

سنت البحرين القانون رقم 30 لعام 2018 فيما يتعلق بحماية البيانات الشخصية في يوليو 2018. ودخل قانون حماية البيانات الشخصية حيز التنفيذ في أغسطس 2019.

التعريفات الرئيسية

- تعريف البيانات الشخصية: يتم تعريف البيانات الشخصية بموجب قانون حماية البيانات الشخصية على أنها أي معلومات من أي شكل تتعلق بفرد يمكن التعرف عليه، أو فرد يمكن تحديد هويته، بشكل مباشر أو غير مباشر، لا سيما من خلال رقم تعريفه الشخصي، أو واحد أو أكثر من معلوماته الجسدية، والفسيولوجية، والفكرية أو الخصائص الثقافية أو الاقتصادية أو الهوية الاجتماعية.
- تعريف البيانات الشخصية الحسّاسة: البيانات الشخصية الحسّاسة هي مجموعة فرعية من البيانات الشخصية. وهي البيانات الشخصية التي تكشف، بشكل مباشر أو غير مباشر، عن الأصل العرقي أو العنصري أو الآراء السياسية أو الفلسفية أو المعتقدات الدينية أو الانتماء النقابي أو السجل الجنائي أو أي بيانات تتعلق بصحتهم أو حياتهم الجنسية. تتطلب البيانات الشخصية الحساسة معالجة أكثر صرامة من قبل مراقبي البيانات.

السلطة

بموجب قانون حماية البيانات الشخصية ستتمتع هيئة حماية البيانات الشخصية (السلطة) بصلاحية التحقيق في انتهاكات قانون حماية البيانات الشخصية من تلقاء نفسها، أو بناءً على طلب الوزير المسؤول، أو ردًا على شكوى. في غضون ذلك، تتولى وزارة العدل مسؤوليات السلطة ريثما يتم تشكيلها.

مسؤولو حماية البيانات

قد يقوم مراقبو البيانات بتعيين مسؤول حماية البيانات اختياريا. كما يجوز لمجلس إدارة السلطة إصدار قرار يلزم فئات معينة من مراقبي البيانات بتعيين مسؤولي حماية البيانات. ومع ذلك، في جميع الحالات، يجب على مراقب البيانات إخطار الهيئة بهذا التعيين في غضون ثلاثة أيام من حدوثه.

التسجيل

يجب على السلطة إنشاء سجل لمسؤولي حماية البيانات. لكي يتم اعتماده كمسؤول حماية بيانات، ينبغي تسجيل الفرد في هذا السجل.

معالجة البيانات

لا يمكن أن تتم معالجة البيانات الشخصية إلا بموافقة صاحب البيانات، ما لم تكن المعالجة ضرورية:

- لتنفيذ عقد يكون صاحب البيانات طرفًا فيه؛
- لاتخاذ خطوات بناءً على طلب صاحب البيانات لإبرام عقد؛
- لحماية المصالح الحيوية لموضوع البيانات؛ أو
- لممارسة المصالح المشروعة لمراقب البيانات أو أي طرف ثالث يتم الكشف عن البيانات له، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية لصاحب البيانات.

يُحظر أيضًا معالجة البيانات الشخصية الحساسة دون موافقة صاحب البيانات، إلا في ظل ظروف محدودة (على سبيل المثال؛ مطلوبة من قبل مراقب البيانات لتنفيذ التزاماتهم، ضرورية لحماية صاحب البيانات، وما إلى ذلك).

حقوق صاحب البيانات

- حق الاعتراض على المعالجة لأغراض التسويق المباشر - الحق في الاعتراض على العملية التي تسبب أضرارًا مادية أو معنوية لمالك المعلومات أو غيره - الحق في الاحتجاج على القرارات التي يتم اتخاذها وفقًا للمعالجة اليدوية - الحق في الاحتجاج للمطالبة بالتعديل والإخفاء والمسح.

نقل البيانات

- يحظر نقل البيانات الشخصية خارج البحرين ما لم يتم النقل إلى دولة أو منطقة توفر حماية كافية للبيانات الشخصية. يجب أن يتم إدراج هذه الدول من قبل السلطة ونشرها في الجريدة الرسمية.
- يمكن لمراقبي البيانات أيضًا نقل البيانات الشخصية إلى البلدان التي لم تُحدّد على أنها تتمتع بحماية كافية للبيانات الشخصية في ظل ظروف معينة بما في ذلك: أن يحدث النقل وفقًا لإذن تصدره السلطة على أساس كل حالة على حدة، إذا وافق صاحب البيانات على هذا النقل، أو أن هناك مصلحة مشروعة وحيوية لعملية النقل، إلخ.

إشعار الخرق

يحتوي قانون حماية البيانات الشخصية على مطلب عام يُلزم مسؤول حماية البيانات بإخطار السلطة بأي خرق بموجب قانون حماية البيانات الشخصية والذي يكون مسؤول حماية البيانات على علم به.

المغــرب

تشريع حماية البيانات

سن المغرب القانون رقم 09-08، في عام 2009 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية.

التعريفات الرئيسية

- تعريف البيانات الشخصية: يتم تعريف البيانات الشخصية على أنها أي معلومات، بغض النظر عن طبيعتها وشكلها، تتعلق بشخص محدد أو يمكن التعرف عليه.
- تعريف البيانات الشخصية الحساسة: يتم تعريف البيانات الشخصية الحساسة بموجب القانون على أنها بيانات شخصية تكشف عن الأصل العرقي أو العنصري، الآراء السياسية، المعتقدات الدينية أو الفلسفية، أو العضوية النقابية للشخص المعني أو تلك المتعلقة بصحته، بما في ذلك بياناته الوراثية.

السلطـة

السلطة المختصة هي اللجنة الوطنية لحماية البيانات.

مسؤولو حماية البيانات

ليس هناك شرط لوجود مسؤول حماية البيانات بموجب قانون حماية البيانات.

التسجيل

تخضع معالجة البيانات الشخصية لإعلان مسبق يتم تقديمه إلى لجنة حماية البيانات الشخصية، وللحصول على إذن مسبق من لجنة حماية البيانات الشخصية عندما تتعلق المعالجة ببيانات حساسة، أو البيانات الجينية، أو البيانات التي تتضمن رقم بطاقة الهوية الوطنية، أو عند استخدام البيانات الشخصية لأغراض أخرى غير تلك التي تم جمعها من أجلها في البداية.

معالجة البيانات

كقاعدة عامة، يجب أن تخضع معالجة البيانات الشخصية لموافقة مسبقة من صاحب البيانات ذات الصلة. ومع ذلك، يمكن إجراء معالجة البيانات الشخصية دون موافقة صاحب البيانات ذات الصلة بشرط أن تكون المعلومات متعلقة بما يلي:

- الامتثال لالتزام قانوني.
- تنفيذ عقد يكون صاحب البيانات ذي الصلة طرفًا فيه أو عند تنفيذ التدابير التعاقدية المسبقة التي يتم اتخاذها بناءً على طلب الأخير.

- حماية المصالح الحيوية لصاحب البيانات ذات الصلة، إذا كان ذلك الشخص غير قادر جسديًا أو قانونيًا على إعطاء موافقته.
- أداء مهمة للمصلحة العامة أو متعلّقة بممارسة السلطة العامة.
- الوفاء بالمصالح المشروعة التي يسعى إليها الشخص المسؤول عن المعالجة أو المتلقي.

حقوق صاحب البيانات

- الحق في أن يتم إعلامه وقت جمع البيانات.
- الحق في عدم تلقّي التسويق المباشر دون موافقته.
- الحق في تقييد أو تصحيح أو حذف البيانات الشخصية.
- الحق في طلب الوصول إلى بياناته الشخصية والمعلومات ذات الصلة حول كيفية / سبب معالجتها.
- الحق في عدم الخضوع لعملية صنع القرار الآلي.

نقل البيانات

يُشترط الحصول على إذن مسبق من اللجنة الوطنية قبل أي نقل للبيانات الشخصية إلى دولة أجنبية. علاوة على ذلك، يمكن للشخص المسؤول عن عملية المعالجة نقل البيانات الشخصية إلى دولة أجنبية فقط إذا كانت الدولة المذكورة تضمن بموجب إطارها القانوني المعمول به مستوى مناسبًا من الحماية للخصوصية والحقوق الأساسية والحريات للأفراد فيما يتعلق بالمعالجة التي تخضع أو قد تخضع لها البيانات، ما لم:

- أعطى صاحب البيانات موافقته الصريحة على النقل.
- النقل والمعالجة اللاحقة مطلوبان لأي مهمة تم تسليط الضوء عليها ضمن الإعفاءات المدرجة في قسم "معالجة البيانات".

إشعار الخرق

لا ينص القانون على أي التزام بإخطار لجنة حماية البيانات الشخصية أو الشخص المعني في حالة حدوث خرق لأمن البيانات.

قطـــر

تشريع حماية البيانات

نفذت قطر القانون رقم (13) لسنة 2016 بشأن حماية البيانات الشخصية. ينص قانون حماية البيانات على أن لكل فرد الحق في خصوصية بياناته الشخصية.

التعريفات الرئيسية

تعريف البيانات الشخصية: يتم تعريف البيانات الشخصية بموجب قانون حماية البيانات على أنها بيانات تتعلق بشخص طبيعي يتم تحديد هويته أو يمكن التعرف عليه بشكل معقول، سواء من خلال هذه البيانات أو عن طريق دمج هذه البيانات مع أي بيانات أو تفاصيل أخرى.

تعريف البيانات الشخصية الحساسة: البيانات الشخصية الحساسة تعني البيانات الشخصية التي تتكون من معلومات تتعلق بالأصل العرقي للشخص الطبيعي، الصحة، الحالة الصحية البدنية أو العقلية، المعتقدات الدينية، العلاقات، والسجلات الجنائية.

السلطـة

وزارة المواصلات والاتصالات القطرية

مسؤولو حماية البيانات

لا يوجد حاليًا أي التزام على المؤسسات في قطر بتعيين مسؤول حماية البيانات. هناك التزام على مراقب البيانات لتحديد المعالجين المسؤولين عن حماية البيانات الشخصية، وتدريبهم بشكل مناسب على حماية البيانات الشخصية وزيادة وعيهم فيما يتعلق بحماية البيانات الشخصية.

التسجيل

لا يوجد حاليا أي متطلبات للتسجيل في قطر.

معالجة البيانات

مراقب البيانات لديه الحرية في معالجة البيانات دون موافقة صاحب البيانات، في الظروف التالية:

- تنفيذ مهمة تتعلق بالمصلحة العامة وفق القانون.
- تنفيذ التزام قانوني أو أمر صادر عن محكمة مختصة.
- حماية المصالح الحيوية للفرد.
- تحقيق أغراض البحث العلمي الجاري تنفيذه للصالح العام.
- جمع المعلومات اللازمة للتحقيق في جريمة جنائية بناء على طلب رسمي من جهات التحقيق.

حقوق صاحب البيانات

- سحب الموافقة على معالجة بياناته الشخصية.
- الاعتراض على أنشطة معالجة معيّنة.
- إصدار طلبات لحذف أو تصحيح بياناته الشخصية.
- طلب الوصول إلى بياناته الشخصية والمعلومات ذات الصلة حول كيفية / سبب معالجتها.
- أن يتم إعلامه عند الكشف عن أي بيانات غير دقيقة تتعلق به.

نقل البيانات

- يُسمح لمراقبي البيانات بجمع ومعالجة ونقل البيانات الشخصية عندما يوافق صاحب البيانات، ما لم يكن ذلك ضروريًا لتحقيق "غرض قانوني" للمراقب أو للطرف الثالث الذي يتم إرسال البيانات الشخصية إليه.
- يجب على مراقبي البيانات عدم اتخاذ تدابير أو اعتماد إجراءات قد تحد من تدفق البيانات عبر الحدود، ما لم تنتهك معالجة هذه البيانات أحكام قانون حماية البيانات أو تتسبب في ضرر جسيم لصاحب البيانات. يعرّف قانون حماية البيانات "تدفق البيانات عبر الحدود" على أنه الوصول إلى البيانات الشخصية، الاطّلاع عليها، استرجاعها واستخدامها أو تخزينها دون قيود حدود الدولة.

إشعار الخرق

يجب على مراقب البيانات إبلاغ عن خرق البيانات الشخصية إلى إدارة الامتثال وحماية البيانات في وزارة النقل والاتصالات دون تأخير وفي غضون 72 ساعة من علمهم بذلك، إذا كان خرق البيانات الشخصية قد يتسبب في إلحاق الضرر بالبيانات الشخصية للأفراد أو خصوصيتهم. يجب على مراقب البيانات إخطار الأفراد بانتهاك البيانات الشخصية دون تأخير وفي غضون 72 ساعة من علمهم إذا كان خرق البيانات الشخصية يمكن أن يتسبب في أضرار جسيمة لبياناتهم الشخصية أو خصوصيتهم.

تـونـــس

تشريع حماية البيانات

ينظم البيانات الشخصية قانون حماية البيانات الشخصية رقم 63 - 2004 المؤرخ في 27 يوليو 2004.

التعريفات الرئيسية

- تعريف البيانات الشخصية: يتم تعريف البيانات الشخصية على أنها جميع المعلومات، بغض النظر عن أصلها أو شكلها، والتي تسمح بشكل مباشر أو غير مباشر بتحديد هوية الشخص الطبيعي أو تحديده، باستثناء المعلومات المتعلقة بالحياة العامة أو التي يعتبرها القانون كذلك.
- تعريف البيانات الشخصية الحساسة: لا يوجد تعريف واضح للبيانات الشخصية الحساسة، ولكن القانون أدرج بعض البيانات الشخصية التي يُحظر معالجتها، أو قد يتطلب الموافقة المسبقة لصاحب البيانات أو تفويض من السلطة الوطنية؛ مثل التاريخ الجنائي والإجراءات، الملاحقة الجنائية، العقوبات، التدابير الوقائية أو التاريخ القضائي، بالإضافة إلى البيانات المتعلقة بالأصول العرقية / الجينية، المعتقدات الدينية، الآراء السياسية، النشاط النقابي / الفلسفي، الصحة والبحث العلمي .

السلطة

تم إنشاء الهيئة الوطنية لحماية البيانات الشخصية (الهيئة) بموجب المرسوم رقم 3003 -2007 المؤرخ في 27 نوفمبر 2007.

مسؤولو حماية البيانات

بموجب القانون التونسي، لا توجد إشارة إلى مسؤولي حماية البيانات.

التسجيل

تخضع أي معالجة للبيانات الشخصية لإعلان مسبق يتم تقديمه في المقر الرئيسي للهيئة الوطنية لحماية البيانات الشخصية، أو عبر أي وسيلة أخرى تترك سجلًا مكتوبًا.

معالجة البيانات

من بين المتطلبات الأساسية للمعالجة المشروعة للبيانات الشخصية موافقة صاحب البيانات، ما يعني أن معالجة البيانات الشخصية لا يمكن أن تتم بدون موافقة خطّية صريحة من صاحب البيانات. تخضع هذه الموافقة للقواعد العامة للقانون إذا كان موضوع البيانات غير كفء أو غير مصرّح به أو غير مؤهّل للتوقيع. بالإضافة إلى ذلك، ولغايات حماية الطفل، وفّر القانون التونسي حماية إضافية للبيانات الشخصية المتعلقة بالأطفال حيث لا يمكن تنفيذ هذا النوع من البيانات دون موافقة وكيل الطفل وبعد إذن من قاضي محكمة الأحداث والأسرة.

حقوق صاحب البيانات

- الحق بإعطاء الموافقة وسحب الموافقة فيما يتعلّق بمعالجة البيانات الشخصية.
- حق صاحب البيانات بالوصول إليها.
- حق الاعتراض على معالجة بيانات شخصية متعلّقة بصاحب البيانات.

نقل البيانات

• يُحظر نقل البيانات الشخصية بشكل عام أو يخضع لتدابير صارمة، بما في ذلك الإذن المسبق (المقدّم إلى الهيئة الوطنية لحماية البيانات الشخصية)، والموافقة الصريحة من الشخص المعني، والتي تُعد إلزامية.

• قد لا يحدث النقل الدولي للبيانات الشخصية إذا لم توفّر الدولة الأجنبية مستوى مناسبًا من الحماية. في كل حالة، يلزم الحصول على إذن الهيئة قبل نقل البيانات الشخصية.

إشعار الخرق

لا توجد التزامات منصوص عليها في القانون بشأن إشعار الخرق.

المُلحق (II) – البيانات الشخصية

أ- بيانات العميل:

1. الأسماء:
   - أ- الاسم الكامل
   - ب- اسم الأم
   - ت- الاسم المستعار (الملقّب بـِ)

2. أرقام التعريف الشخصية:

   - أ- رقم التأمين القومي أو الاجتماعي
   - ب- رقم جواز السفر
   - ت- رقم تصريح الإقامة
   - ث- رقم تصريح التأشيرة
   - ج- رقم رخصة القيادة
   - ح- رقم التعريف الضريبي
   - خ- أرقام التعريف الحكومية الأخرى

3. بيانات مالية شخصية

   - أ- رقم الحساب أو رقم هوية العميل (رقم تعريف مخصص لشخص واحد)
   - ب- رقم صندوق الأمانات
   - ت- رقم بطاقة الائتمان/الخصم
   - ث- رقم الحساب المصرفي الدولي IBAN
   - ج- رموز التعريف الشخصي المُستخدمة للسماح بالاستخدام الإلكتروني لبطاقة المعاملات المالية

4. معلومات العنوان الشخصي:

   - أ- عنوان المنزل
   - ب- العنوان البريدي (ص.ب./ الرمز البريدي)
   - ت- عنوان البريد الإلكتروني
   - ث- عنوان بروتوكول الإنترنت

5. أرقام الهاتف الشخصية:
   - أ- أرقام هاتف المنزل
   - ب- أرقام الهاتف المحمول

6. البيانات البيومترية – **فئة خاصة/بيانات حساسة**

   - أ- التعرّف على وريد الإصبع - **فئة خاصة/بيانات حساسة**
   - ب- التوقيعات الرقمية

ت- هندسة الوجه – **فئة خاصة/بيانات حساسة**
ث- الصور الفوتوغرافية (خاصة للوجه أو الخصائص المميّزة الأخرى)

7.أرقام حسابات الإنترنت، أو أسماء تعريف الأنترنت:

أ- أسماء تسجيل الدخول
ب- معرّفات وسائل التواصل الاجتماعي (مثلاً، فايس بوك، تويتر، لينكد إن)

8. معلومات عن المركبة
أ- رقم تسجيل المركبة
ب- رقم لوحة ترخيص المركبة

ب - الموظفون

1. بيانات السيرة الذاتية
2. بيانات تحديد تردد الراديو (بطاقة / شارة الدخول) – **فئة خاصة/ بيانات حساسة**
3. تصريح أمني
4. معلومات مالية
5. السجل الجنائي - **فئة خاصة/ بيانات حساسة**
6. عنوان المنزل
7. معلومات التظلم - **فئة خاصة / بيانات حساسة**
8. السجلاّت التأديبية
9. سبب إجازة الغياب
10. معلومات الرواتب والمزايا
11. معلومات التوظيف
12. معلومات تربوية
13. معلومات صحية - **فئة خاصة / بيانات حساسة**

المُلحق (III) استبيان تقييم الخصوصية وحماية البيانات لمجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا

الرجوع إلى موقع المجموعة الإلكتروني: أدوات الامتثال

MENA FCCG website / Compliance Tools at:
http://menafccg.com/publications/

عن مجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا

مجموعة الامتثال لمكافحة الجرائم المالية في منطقة الشرق الأوسط وشمال أفريقيا هي هيئة تطوعية تسعى لتحقيق عمل جماعي في مكافحة غسل الأموال وتمويل الإرهاب في المنطقة. تضم المجموعة ١٣ مصرفاً من تسعة بلدان في منطقة الشرق الأوسط وشمال إفريقيا، بما في ذلك ؛ البحرين ومصر والأردن والكويت ولبنان وعمان وقطر والمملكة العربية السعودية والإمارات العربية المتحدة.

www.menafccg.com
تُرسل الاستفسارات إلى
info@menafccg.com