

الملحق (أ): قائمة التحقق من الامتثال

يُطبق على شركات التدقيق الخارجي المعتمدة التي ستقوم بإجراء تقييم الامتثال لمتطلبات حماية البيانات الشخصية وفقاً لقانون حماية البيانات الشخصية ولائحته التنفيذية

البند	معيّار الامتثال	الأدلة
السجل التجاري	يجب أن يكون لدى المدقق الخارجي سجل تجاري ساري المفعول في سلطنة عُمان، على أن تكون الشركة مسجلة قانونياً في السلطنة منذ مدة لا تقل عن 12 شهراً، مع الالتزام بجميع القوانين والأنظمة المحلية المتعلقة بحماية البيانات الشخصية.	- تقديم نسخة من: - شهادة السجل التجاري (CR). - تقديم ما يثبت أن الشركة مسجلة في سلطنة عُمان منذ مدة لا تقل عن 12 شهراً.
الشهادات	يجب أن تمتلك الشركة شهادات معترف بها مثل ISO/IEC 27001 و ISO/IEC 27701	- تقديم نسخ من الشهادات التالية وتكون سارية المفعول: - ISO/IEC 27001 - ISO/IEC 27701
الفريق الفني المتخصص	يجب أن يكون المدقق الرئيسي حاصلاً على شهادة واحدة على الأقل في مجال أمن المعلومات أو في مجال التدقيق، أو في مجال الخصوصية أو حماية البيانات.	- تقديم قائمة بأعضاء الفريق الفني وسيرهم الذاتية. - وصف الأدوار الوظيفية لكل عضو في الفريق (مثل: مدير المشروع، المدقق الرئيسي). - يجب أن يكون للمدقق الرئيسي خبرة مهنية لا تقل عن ثلاث سنوات. - يجب أن يكون المدقق الرئيسي حاصلاً على واحدة على الأقل من الشهادات التالية: - المدير التنفيذي المعتمد لأمن المعلومات (CCISO). - أخصائي نظم المعلومات الأمنية المعتمد (CISSP). - مدقق نظم المعلومات المعتمد (CISA). - مدير أمن المعلومات المعتمد (CISM). - مراجع رئيسي (ISO/IEC 27001:2022) - أخصائي الخصوصية المعتمد (CIPP).
خبرة التدقيق	يجب أن يكون للمدقق الخارجي خبرة موثوقة ومثبتة في تقديم خدمات التدقيق أو تقييم الامتثال في مجالات حماية البيانات الشخصية أو خصوصية البيانات أو أمن المعلومات أو المجالات ذات الصلة.	- تقديم قائمة بمشاريع التدقيق السابقة - بيان بعدد سنوات الخبرة.



الملحق (أ): قائمة التحقق من الامتثال

يُطبق على شركات التدقيق الخارجي المعتمدة التي ستقوم بإجراء تقييم الامتثال لمتطلبات حماية البيانات الشخصية وفقاً لقانون حماية البيانات الشخصية ولائحته التنفيذية

• تقديم نموذج لخطّة التدقيق يغطي جميع المراحل الثلاث (التخطيط، التنفيذ، إعداد التقارير). • تقديم نموذج لتقرير التدقيق.	يجب توثيق جميع مراحل التدقيق بشكل كامل، بما يشمل التخطيط والتنفيذ وإعداد التقارير.	توثيق إجراءات التدقيق
○ تقديم سياسة الاحتفاظ بالسجلات. ○ تقديم مستندات رسمية توضح أن مدة الاحتفاظ لا تقل عن خمس سنوات.	يجب الاحتفاظ بسجلات التدقيق لمدة لا تقل عن خمس سنوات.	سياسة حفظ السجلات
○ سياسات داخلية متوافقة مع القوانين مثل (قانون حماية البيانات الشخصية). ○ تأكيد على وجود وحدة امتثال ومسؤول حماية البيانات معين.	يجب أن تلتزم الشركة بالقوانين المحلية المتعلقة بحماية البيانات الشخصية.	التقيد بالقوانين
○ سياسة حماية البيانات الداخلية. ○ التحقق من تطبيق ضوابط الأمان مثل (التشفير، الوصول المصرح به، وغيرها). ○ تقارير الاختبارات الأمنية (مثل: اختبارات الاختراق).	يجب أن تتبع الشركة إجراءات واضحة لحماية البيانات ومنع الوصول غير المصرح به	سياسة حماية البيانات والسرية
○ قائمة بأعضاء الفريق الفني مع توضيح جنسيتهم والتفاصيل الوظيفية. ○ سجلات التوظيف أو عقود العمل التي تثبت تحقيق نسبة التعمين المطلوبة.	يجب أن يتكون الفريق الفني من نسبة لا تقل عن 30% من المواطنين العمانيين.	التعمين

الملحق (ب): قائمة التحقق من الامتثال

يُطبق على شركات التدقيق الخارجي المعتمدة التي ستقوم بإجراء تقييم الامتثال لمتطلبات حماية البيانات الشخصية وفقا لقانون حماية البيانات الشخصية ولائحته التنفيذية

البند	الادلة
سياسة حماية البيانات الشخصية	مستند سياسة حماية البيانات الشخصية المعتمدة من قبل المتحكم وفقا للضوابط المحددة في المعيار.
حقوق صاحب البيانات الشخصية	نموذج الموافقة على معالجة البيانات الشخصية مستند ضوابط وإجراءات تمكين صاحب البيانات الشخصية من ممارسة حقوقه.
تصريح معالجة البيانات الشخصية	تصريح حماية البيانات الشخصية.
معالجة البيانات الشخصية للطفل	نموذج الموافقة الصريحة لولي أمر الطفل أو من في حكمه لمعالجة البيانات الشخصية للطفل أو من في حكمه. الوسائل المحددة من قبل المتحكم أو المعالج لتمكين ولي أمر الطفل من الوصول إلى البيانات الشخصية لطفله لتحديثها وتعديلها. نموذج موافقة ولي الأمر في حال الإفصاح عن البيانات الشخصية لطفله.
المواد الإعلانية / التسويقية / الأغراض التجارية	مستند يثبت التزام المتحكم بضوابط إرسال المواد الإعلانية أو التسويقية أو ذات الأغراض التجارية.
النشر / المشاركة / الإفصاح عن البيانات الشخصية المنصوص عليها في المادة (5) من قانون حماية البيانات الشخصية:	مستند يثبت أن نشر أو مشاركة أو الإفصاح عن البيانات الشخصية يتم وفقا للحالات والحدود المقررة قانونا أو تنفيذا لحكم أو قرار قضائي.
سرية البيانات الشخصية:	مستند يثبت الآتي: • وضع واستخدام وتفعيل الأنظمة الإلكترونية من الوصول غير المشروع للبيانات الشخصية أو تسريبها أو العبث بها أو إساءة استخدامها. • وضع أنظمة استعادة البيانات الشخصية عند وقوع حادث مادي أو تقني. • وجود عمليات اختبار لفعالية الإجراءات التقنية الموجودة لديه.
الاحتفاظ بسجلات معالجة البيانات الشخصية:	تحديد مدة زمنية للاحتفاظ بسجلات معالجة البيانات الشخصية تتناسب مع الغرض والمعالجة. تحديد سبب الاحتفاظ بهذه السجلات (محددا ومشروعا) مع توفير أنظمة الحماية الفنية للاحتفاظ بمستندات المعالجة.

الملحق (ب): قائمة التحقق من الامتثال

يُطبق على شركات التدقيق الخارجي المعتمدة التي ستقوم بإجراء تقييم الامتثال لمتطلبات حماية البيانات الشخصية وفقاً لقانون حماية البيانات الشخصية ولائحته التنفيذية

سجل أنشطة معالجة البيانات الشخصية	سجل أنشطة معالجة البيانات الشخصية.
اختراق البيانات الشخصية:	مستند يتضمن وجود التدابير والإجراءات المتبعة قبل حدوث الاختراق وأثناء حدوثه والإجراءات التصحيحية المتخذة لاحقاً.
مسؤول حماية البيانات الشخصية:	استمارة تعيين مسؤول حماية بيانات شخصية.
نقل وتحويل البيانات الشخصية خارج الحدود:	مستند يثبت أخذ الموافقة الصريحة من صاحب البيانات الشخصية قبل نقل أو تحويل بياناته خارج الحدود. (في حال عدم انطباق إحدى حالات النقل بدون أخذ الموافقة الصريحة). تقرير تقييم مستوى المخاطر عند نقل البيانات الشخصية خارج الحدود.