الملحق (أ): 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	معيار الامتثال	الادلة
التسجيل القانوني	يجب أن يكون لدى المدقق الخارجي سجل تجاري ساري المفعول في سلطنة عُمان، يشمل نشاط **التدقيق الخارجي في مجال حماية البيانات الشخصية** (رقم النشاط 620209)، مع الالتزام بجميع القوانين والأنظمة المحلية المتعلقة بحماية البيانات الشخصية.	• تقديم نسخة من: o شهادة السجل التجاري(CR) . o نشاط **التدقيق الخارجي في مجال حماية البيانات الشخصية** (رقم النشاط 620209).
الشهادات المعتمدة	يجب أن تمتلك الشركة شهادات معترف بها مثل ISO/IEC 27001 و ISO/IEC 27701	• تقديم نسخ من الشهادات: o ISO/IEC27001 o ISO/IEC 27701
القدرة الفنية للفريق	يجب أن يكون المدقق الرئيسي حاصلًا على شهادة واحدة على الأقل في مجال أمن المعلومات وحوكمة البيانات، أو في مجال الخصوصية وحماية البيانات.	• تقديم قائمة بأعضاء الفريق الفني وسيرهم الذاتية. • وصف الأدوار الوظيفية لكل عضو في الفريق (مثل: مدير المشروع، المدقق الرئيسي). • يجب أن يكون المدقق الرئيسي حاصلًا على واحدة على الأقل من الشهادات التالية: o المدير التنفيذي المعتمد لأمن المعلومات (**CCISO**). o أخصائي نظم المعلومات الأمنية المعتمد (**CISSP**). o مدقق نظم المعلومات المعتمد (**CISA**). o مدير أمن المعلومات المعتمد (**CISM**). o مراجع رئيسي (**ISO/IEC 27001:2022**) o أخصائي الخصوصية المعتمد (**CIPP**).
الخبرة في التدقيق	يجب أن تمتلك الشركة خبرة مثبتة في تدقيق حماية البيانات الشخصية.	• تقديم قائمة بمشاريع التدقيق السابقة • بيان بعدد سنوات الخبرة.
إجراءات التدقيق والتوثيق	يجب توثيق جميع مراحل التدقيق بشكل كامل، بما يشمل **التخطيط والتنفيذ وإعداد التقارير**.	• تقديم نموذج لخطة التدقيق يغطي جميع المراحل الثلاث (التخطيط، التنفيذ، إعداد التقارير). • تقديم نموذج لتقرير التدقيق.

الملحق (أ): 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

حفظ السجلات	يجب الاحتفاظ بسجلات التدقيق لمدة لا تقل عن خمس سنوات.	○ تقديم سياسة الاحتفاظ بالسجلات. ○ تقديم مستندات رسمية توضح أن مدة الاحتفاظ لا تقل عن خمس سنوات.
الامتثال للقوانين	يجب أن تلتزم الشركة بالقوانين المحلية المتعلقة بحماية البيانات الشخصية.	○ سياسات داخلية متوافقة مع القوانين مثل (قانون حماية البيانات الشخصية). ○ تأكيد على وجود وحدة امتثال ومسؤول حماية البيانات معين.
حماية البيانات	يجب أن تتبع الشركة إجراءات واضحة لحماية البيانات ومنع الوصول غير المصرح به	○ سياسة حماية البيانات الداخلية. ○ التحقق من تطبيق ضوابط الأمان مثل (التشفير، الوصول المصرح به، وغيرها). ○ تقارير الاختبارات الأمنية (مثل: اختبارات الاختراق).
التعمين	يجب أن يتكون الفريق الفني من نسبة لا تقل عن 30% من المواطنين العمانيين.	○ قائمة بأعضاء الفريق الفني مع توضيح جنسيتهم والتفاصيل الوظيفية. ○ سجلات التوظيف او عقود العمل التي تثبت تحقيق نسبة التعمين المطلوبة.

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 تتضمن على الأقل: حقوق صاحب البيانات الشخصية، وكيفية المعالجة وان يتم وضعها في مكان ظاهر يمكن صاحب البيانات الشخصية من الاطلاع عليها.
حقوق صاحب البيانات الشخصية	مستند يوفر آلية واضحة لاستيفاء الموافقة الكتابية الصريحة لصاحب البيانات الشخصية وتمكينه من ممارسة حقوقه الآتية: • إلغاء موافقته على معالجة بياناته الشخصية وذلك مع عدم الإخلال بالمعالجات التي تمت قبل الإلغاء وطلب تعديل بياناته الشخصية أو تحديثها أو حجبها. • الحصول على نسخة من بياناته الشخصية المعالجة. • نقل بياناته الشخصية إلى متحكم آخر. • طلب محو بياناته الشخصية مالم تكن تلك المعالجة ضرورية لأغراض الحفظ والتوثيق الوطنية. • إخطاره بأي اختراق أو انتهاك لبياناته الشخصية وما تم اتخاذه من إجراءات في هذا الشأن.
تصريح معالجة البيانات الشخصية	تصريح حماية البيانات الشخصية.
معالجة البيانات الشخصية للطفل	مستند سواء كان ورقي أو إلكتروني يثبت الحصول على الموافقة الصريحة لولي الأمر ومستند آخر يفيد ما يثبت التقيد بضوابط معالجة البيانات الشخصية للطفل.
المواد الإعلانية / التسويقية / الأغراض التجارية	مستند يثبت الآتي: • الحصول على الموافقة الكتابية لصاحب البيانات الشخصية. • إخطار صاحب البيانات الشخصية بوسيلة المواد الإعلانية أو التسويقية أو التجارية. • تحديد آلية إيقاف استقبال المواد الإعلانية أو التسويقية أو التجارية. • التوقف عن إرسال المواد الإعلانية أو التسويقية أو التجارية فور تلقي طلب الإيقاف من صاحب البيانات الشخصية وبدون مقابل).
النشر / المشاركة / الإفصاح عن البيانات الشخصية المنصوص عليها في المادة (5) من قانون حماية البيانات الشخصية:	مستند يثبت النشر أو المشاركة أو الإفصاح عن البيانات الشخصية المنصوص عليها في المادة (5) من قانون حماية البيانات الشخصية وفقا للحدود والحالات المقررة قانونا أو إذا كان تنفيذا لحكم أو قرار قضائي).

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

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:	مستند يثبت مراعاة الضوابط الآتية: • أن يكون سبب الاحتفاظ بمستندات عمليات المعالجة محددا ومشروعا. • أن يتم تحديد مدة زمنية للاحتفاظ تتناسب مع الغرض من المعالجة. • أن يوفر أنظمة الحماية الفنية للاحتفاظ الأمن بمستندات المعالجة.
اختراق البيانات الشخصية:	مستند يفيد التدابير والإجراءات المتبعة قبل حدوث الاختراق وأثناء حدوثه والإجراءات التصحيحية المتخذة لاحقا.
مسؤول حماية البيانات الشخصية:	مستند يثبت تحديد مسؤول حماية البيانات الشخصية وفقا للاستمارة المعدة لذلك مع مراعاة الآتي: • أن يكون مؤهلا للقيام بالمهام الواردة في المادة (35) من اللائحة التنفيذية والتي تتمثل في: • تقديم المقترحات والاستشارات للمتحكم أو المعالج فيما يتعلق بالتزاماتهما الواردة في القانون واللائحة • متابعة تنفيذ سياسات المتحكم أو المعالج المتعلقة بحماية البيانات الشخصية. • متابعة تنفيذ المتحكم أو المعالج لالتزاماته المنصوص عليها في القانون واللائحة. • التنسيق مع الإدارة المختصة في المسائل المتعلقة بمعالجة البيانات الشخصية. يجب تمكين صاحب البيانات الشخصية من حقه في الاتصال بمسؤول حماية البيانات الشخصية في كل المسائل المتعلقة بمعالجة بياناته الشخصية.
نقل وتحويل البيانات الشخصية خارج الحدود:	مستند يثبت الموافقة الصريحة لصاحب البيانات الشخصية مع الأخذ بعين الاعتبار ألا يترتب على نقل البيانات أو تحويلها مساس بالأمن الوطني أو المصالح العليا للدولة. مستند يثبت أن لدى جهة المعالجة الخارجية قدر كافي من الحماية للبيانات الشخصية لا يقل عن مستوى الحماية المقررة في القانون واللائحة + تقرير مستوى الحماية لدى جهة المعالجة الخارجية.