سياسة حماية البيانات الشخصية

خصائص المستند

اسم المستند	سياسة حماية البيانات الشخصية
المؤسسة	جامعة تبوك
مالك الوثيقة	مكتب إدارة البيانات
رقم الاصدار	1.0
الحالة	اصدار
تاريخ الإصدار	11 يناير 2024
التصنيف الأمني	داخلي

تاريخ التعديلات

الاصدار	التاريخ	التعديلات	تحرير	مراجعة	موافقة
1.0	11 يناير 2024	لا يوجد	د.مريم الشهري	د.محمد العتيبي	لجنة التحول الرقمي

الموافقات

الاسم	الوظيفة	التاريخ	التوقيع
د.محمد متعب العتيبي	مدير مكتب إدارة البيانات	11 يناير 2024	
أعضاء لجنة التحول الرقمي	اللجنة الدائمة للتحول الرقمي	15 فبراير 2024	محضر الاجتماع

جدول التعريفات

المصطلح	التعريف
الجامعة	جامعة تبوك
إدارات الأعمال	الوكالات، العمادات، الوحدات، الإدارات، الأقسام.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة، مثل: الأرقام، أو الحروف، أو الصور الثابتة، أو الفيديو، أو التسجيلات الصوتية، أو الرموز التعبيرية.
البيانات الشخصية	كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلًا للتعرف عليه بصفة مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك -على سبيل المثال لا الحصر - الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، والبيانات الصحية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي أو ذات السمة الخاصة التي يستدل منها على فرد معين.

الوصول للبيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجامعة، لغرض استخدامها.
صاحب البيانات الشخصية	الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.
معالجة البيانات الشخصية	جميع العمليات التي تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، وتشمل هذه العمليات -على سبيل المثال لا الحصر- جمع البيانات ونقلها وحفظها وتخزينها ومشاركتها وإتلافها وتحليلها واستخراج أنماطها والاستنتاج منها وربطها مع بيانات أخرى.
الافصاح عن البيانات الشخصية	تمكين أي شخص – ماعدا مكتب إدارة البيانات في الجامعة - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها أو الوصول إليها بأي وسيلة ولأي غرض.
تسريب البيانات الشخصية	الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواءً بقصد أو بغير قصد.
اتلاف البيانات الشخصية	أي عمل يؤدي إلى إزالة البيانات الشخصية ويجعل من المتعذر الاطلاع عليها أو استعادتها مرة أخرى، بما في ذلك المسح والحذف سواءً كان ذلك إلكترونيًا أو ماديًا.
إشعار الخصوصية	هو بيان خارجي موجه للأفراد يوضح محتوى البيانات الشخصية ووسائل جمعها والغرض من معالجتها وكيفية استخدامها والجهات ذات العلاقة التي سيتم مشاركة هذه البيانات معها وفترة الاحتفاظ بها وآلية التخلص منها.
مستويات تصنيف البيانات	مستويات تصنيف البيانات هي: سري للغاية، سري، مقيد، عام.

Error! Bookmark not defined.

1.1	1.23	1.34	1.44 1.54	.42
	بنود السياسة		8	
2.1	2.25	2.35	2.46 2.56	.83
	الوثائق ذات العلاقة		12	

1. المقدمة

1.1 الغرض من الوثيقة

استجابة لضوابط مكتب إدارة البيانات الوطنية والمعايير ذات الصلة بضرورة وضع سياسات حوكمة البيانات في الجهات الحكومية انطلاقًا من سياسات حوكمة البيانات الوطنية التي تم تطويرها، قام مكتب البيانات في الجامعة بتطوير وثيقة سياسة حماية البيانات الشخصية، بالتوافق مع سياسات مكتب إدارة البيانات الوطنية.

الغرض من هذه السياسة هو تقديم التزام الجامعة بخصوصية البيانات الشخصية للمستفيد وحمايتها.

تهدف هذه السياسة إلى وضع القواعد الأساسية لحماية البيانات الشخصية التي يتم معالجتها والتي يجب اتباعها من قبل إدارات الأعمال داخل الجامعة لضمان سلامة البيانات الشخصية لدى المستخدمين.

1.2 نطاق عمل السياسة وتطبيقها

تطبق هذه السياسة على جميع جهات الجامعة التي تتعامل بشكل مباشر أو غير مباشر مع البيانات الشخصية لكافة منسوبي ومنسوبات الجامعة (عضو / عضوة، موظف / موظفة، طالب / طالبة)، وغيرهم ممن يرتبط بعلاقة تعاقدية أو نظامية مع الجامعة.

لا تنطبق أحكام هذه السياسة في الحالات التالية:

- تحقيق متطلبات نظامية وفق الأنظمة واللوائح والسياسات المعمول بها.
- استيفاء متطلبات قضائية.
- تنفيذ التزام بموجب اتفاق تكون المملكة طرفًا فيه.
- حماية الصحة، أو السلامة العامة، أو حماية المصالح الحيوية للأفراد.

1.3 جدول مراجعة السياسة

ينبغي مراجعة هذه السياسة بشكل منتظم بحيث تكون هذه المراجعة مرة واحدة سنويًا على أقل تقدير وفقًا لما يوجه به المشرف العام على السياسة.

1.4 مراقبة الامتثال

يقاس الامتثال لسياسة حماية البيانات الشخصية وفقًا لمعايير ومؤشرات الأداء الموضوعة من مكتب إدارة البيانات في الجامعة وبالتوافق مع متطلبات مكتب إدارة البيانات الوطنية، ويتم مراجعة معايير الامتثال بشكل دوري من قبل مدير مكتب إدارة البيانات.

1.5 مصفوفة الأدوار والمسؤوليات

اللجنة التوجيهية	اعتماد السياسة والخطط واتخاذ القرارات لحل المشاكل وحالات التصعيد.
مكتب وحدة حوكمة البيانات	مكتب وحدة حوكمة البيانات هو الجهة المسؤولة عن إعداد سياسة وإجراءات حماية البيانات الشخصية في الجامعة بما ينسجم مع ما يصدره مكتب إدارة البيانات الوطنية ويشمل ذلك: - إعداد وتحديث سياسة حماية البيانات الشخصية. - إعداد وتحديث واعتماد إشعار الخصوصية لاستخدامه من قبل إدارات الأعمال التي تتعامل مع البيانات الشخصية. - الإشراف على تحديد البيانات الشخصية التي تتعامل معها الجامعة بالمشاركة مع إدارات الأعمال في الجامعة. - اعتماد خطة وآلية تطبيق سياسة حماية البيانات الشخصية. - إعداد تقارير الامتثال لسياسة حماية البيانات الشخصية في الجامعة لأصحاب المصلحة. - إعداد برامج التوعية لرفع مستوى الوعي وتعزيز ثقافة حماية البيانات الشخصية.

	- الاطلاع على طلبات مشاركة البيانات المرسلة من الجهات المختلفة وتوجيهها لممثلي بيانات الأعمال والتحقق من أنّ البيانات المطلوبة مصنفة.
إدارات الأعمال	تطبيق سياسة حماية البيانات الشخصية وذلك من خلال: - التعاون مع مكتب إدارة البيانات لتحديد مرجعية البيانات الشخصية في الجامعة. - الالتزام بتطبيق سياسة البيانات الشخصية وإشعارات الخصوصية.
قطاع الاستراتيجية (عمادة التطوير والجودة)	مراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجهة.
عمادة تقنية المعلومات	تتولى إدارات تقنية المعلومات تطبيق بنود السياسة على كافة الأنظمة وقواعد البيانات.
إدارة الأمن السيبراني	تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المرتبطة بحماية البيانات الشخصية بما ينسجم مع ما تصدره الهيئة الوطنية للأمن السيبراني. ويشمل ذلك: - متابعة وتدقيق أعمال تطبيق ضوابط الحماية على البيانات الشخصية. - إعداد التقارير لأصحاب المصلحة والتصعيد بما يخص تطبيق ضوابط الحماية على البيانات الشخصية ومشاركة التقارير مع مكتب إدارة البيانات.
إدارة المخاطر	تقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وتحديد مستوى قبول المخاطر وإقرارها على مستوى الجامعة ومشاركة نتائج التقييم مع مكتب البيانات البلدية وأصحاب المصلحة في القطاع.
الإدارة القانونية	تقديم الاستشارات فيما يتعلق بالإشعارات أو القضايا المتعلقة بتسريب البيانات الشخصية، ومراجعة الصيغ القانونية لإشعار الخصوصية والعقود، وحقوق أصحاب البيانات.

2. بنود السياسة

2.1 المسؤوليات

2.1.1 تتم مراجعة إدارات الأعمال المسؤولة داخل الجامعة عن تطبيق هذه السياسة وضمان فهم الموظفين لها وأدائهم للعمليات والإجراءات اللازمة لتنفيذها وفقًا لضوابط محددة يتم تعريفها من قبل مكتب إدارة البيانات.

2.1.2 يكون مكتب ادارة البيانات مسؤولًا عن التدقيق على الامتثال لهذه السياسة والضوابط وتقديم تقرير التدقيق مع التوصيات لتتم مراجعته من قبل لجنة حوكمة البيانات للتصديق والموافقة.

2.2 القواعد الأساسية لحماية البيانات الشخصية

2.2.1 أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بالجامعة واعتمادها من قبل معالي مدير الجامعة (أو من يفوضه) ونشرها إلى جميع الأطراف المعنية بتطبيقها.

2.2.2 أن يتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل، أو الوصول غير المصرّح به – وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

2.2.3 أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالجامعة– إشعار الخصوصية – يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.

2.2.4 أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية أو الصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.

2.2.5 أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكّن من تحقيق الأغراض المحددة في إشعار الخصوصية.

2.2.6 أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضروريًا لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح، وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرّح به نظامًا.

2.2.7 أن يتم تحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.

2.2.8 أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة.

2.2.9 أن يتم الاحتفاظ بالبيانات الشخصية بعد التحقق من دقتها واكتمالها وحداثتها، كما يجب أن تكون هذه البيانات ذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

2.2.10 أن يتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

2.3 حقوق صاحب البيانات

- أولاً: الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألّا تعالج بياناته لاحقًا بصورة تتنافى مع الغرض من جمعها والذي من أجله قدّم موافقته الضمنية أو الصريحة.
- ثانياً: الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت - مالم يكن هناك متطلبات نظامية أو قضائية تتطلب عكس ذلك.
- ثالثاً: الحق في الوصول إلى بياناته الشخصية في الجامعة، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

2.4 الأدوار والمسؤوليات

2.4.1 يتولّى مكتب ادارة البيانات إعداد وتطبيق ونشر السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، وتكون اللجنة التنفيذية لإدارة وحوكمة البيانات مسؤولة عنها واعتمادها ويكون معالي مدير الجامعة – مسؤول عن الموافقة عليها واعتمادها.

2.4.2 أن يقوم مكتب إدارة البيانات بالتعاون مع إدارات الأعمال بتحديد مرجعية البيانات الشخصية داخل الجامعة والذي بدوره يقوم بالموافقة على استخدام ومعالجة البيانات الشخصية.

2.4.3 يتولّى مكتب إدارة البيانات وضع سياسات لإدارة دورة حياة البيانات الشخصية من الإنشاء حتى الإتلاف ويشمل في ذلك توصيفها ونمذجتها وتجويدها وتكاملها وطريقة حمايتها إداريًا وتنفيذيًا وطرق وقنوات الوصول إليها.

2.4.4 يقوم مكتب ادارة البيانات بالتعاون مع إدارات الأعمال ذات الصلة وإدارات المخاطر والأمن السيبراني بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على معالي مدير الجامعة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.

2.4.5 يكون مكتب ادارة البيانات مسؤول عن تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالجامعة، على أن تتضمن مهام ومسؤوليات المكتب- وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.

2.4.6 تقوم إدارة العقود، عمادة الموارد البشرية، عمادة القبول والتسجيل، عمادة البحث العلمي، المراكز البحثية وغيرها من الجهات التي تتعامل مع جهات خارجية بمراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة.

2.4.7 يقوم مكتب إدارة البيانات بإعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الجهة التنظيمية والمكتب حسب التسلسل الإداري -بناءً على قياس شدة الأثر.

2.4.8 يقوم مكتب إدارة البيانات بإعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقًا لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجامعة.

2.4.9 التحقق من إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي/الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح، يشمل ذلك كل قنوات تقديم الخدمة والتواصل مع المستفيدين.

2.4.10 التحقق من إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى)، يشمل ذلك كل قنوات تقديم الخدمة والتواصل مع المستفيدين.

2.4.11 يجب تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال (Preferences, Opt-in and Opt-out).

2.4.12 يتولى مسؤولو التواصل أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.

2.4.13 يجب أن تتضمن القنوات الرقمية نماذج تضمن أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.

2.4.14 التأكد من أن يكون الغرض من جمع البيانات متوافقًا مع الأنظمة وذو علاقة مباشرة بنشاط الجامعة.

2.4.15 التأكد من أن يكون محتوى البيانات مقتصرًا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.

2.4.16 التأكد من تقييد جمع البيانات على المحتوى المعد سلفًا يكون بطريقة عادلة مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل.

2.4.17 التأكد من استخدام البيانات على الغرض التي جُمعت من أجله.

2.4.18 التأكد من تخزين البيانات الشخصية ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد حصول جهة التحكم على موافقة كتابية من الجهة التنظيمية، بعد تنسيق الجهة التنظيمية مع المكتب.

2.4.19 يقوم مكتب وحدة حوكمة البيانات بإعداد وتوثيق سياسة وإجراءات التخلص من البيانات لإتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به – وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية – وذلك وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني وما جاء في سياسة الاحتفاظ بالبيانات والتخلص منها لإدارة البيانات لدى الجامعة.

2.4.20 يقوم مكتب ادارة البيانات بتضمين أحكام سياسة الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى وفقًا لما جاء في السياسة العامة لإدارة البيانات لدى الجامعة.

2.4.21 تحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.

2.4.22 التحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقًا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

2.4.23 يتأكد مكتب وحدة حوكمة البيانات من حظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقًا للأغراض المحددة بعد موافقة صاحب البيانات ووفقًا للأنظمة واللوائح على أن يتم تزويد الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة وتضمينها في العقود والاتفاقيات.

2.4.24 يقوم مكتب وحدة حوكمة البيانات بإعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله، تضامنًا مع سياسة جودة البيانات بمكتب إدارة البيانات في الجامعة.

2.4.25 استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الجامعة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال لا الحصر:

- منح صلاحيات الوصول إلى البيانات وفقًا لمهام ومسؤوليات العاملين بطريقة تحول دون تداخل الاختصاص وتتلافى تشتيت المسؤوليات.
- تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفر إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).
- توقيع العاملين الذين يباشرون عمليات معالجة البيانات على تعهد للمحافظة على البيانات وعدم الإفصاح عنها الا وفقًا للسياسات، والإجراءات، والأنظمة، واللوائح.
- اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقًا لطبيعة وحساسية البيانات وسياسة الوصول المعتمدة من قبل الجهة.
- استخدام التدابير الأمنية المناسبة – كالتشفير، وعزل بيئة التطوير والاختبار عن بيئة التشغيل – لأمن البيانات الشخصية وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

2.4.26 تكون مسؤولية مكتب إدارة البيانات مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على معالي مدير الجامعة – أو من يفوضه – كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار الجهة التنظيمية والمكتب حسب التسلسل التنظيمي.

2.5 أحكام عامة

- أولاً: يجب التنسيق مع الجهات التنظيمية التي تتولى مواءمة أحكام سياسات حوكمة البيانات الوطنية مع وثائقها التنظيمية وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه القواعد الاسترشادية.
- ثانياً: يجب التنسيق مع الجهات التنظيمية التي تتولّى مراقبة الامتثال للمبادئ الأساسية والقواعد الاسترشادية لسياسات حوكمة البيانات الوطنية بشكل دوري.
- ثالثاً: يجب الامتثال لهذه المبادئ الأساسية والقواعد الاسترشادية وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.
- رابعاً: يجب إبلاغ الجهات التنظيمية فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية.
- خامساً: عند التعاقد مع جهات المعالجة يجب التحقق بشكل دوري من امتثال جهات المعالجة لهذه المبادئ الأساسية والقواعد الاسترشادية وفقاً للآليات والإجراءات التي تحددها الجهات التنظيمية، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها جهات المعالجة.
- سادساً: يمارس المكتب أدوار ومهام الجهات التنظيمية على جهات التحكم غير الخاضعة لجهات تنظيمية.
- سابعاً: يحق للجهات التنظيمية وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع المكتب.
- ثامناً: تقوم الجهات التنظيمية – بعد التنسيق مع المكتب – بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي.
- تاسعاً: يقوم المكتب بوضع المعايير اللازمة التي تساعد جهات التحكم على معرفة ما إذا كان تعيين مسؤول حماية بيانات يعتبر متطلب أساسي أو اختياري.

3. الوثائق ذات العلاقة

- سياسة تعريف وتصنيف البيانات
- سياسة استخدام البيانات
- سياسة حماية البيانات الشخصية – مكتب إدارة البيانات الوطنية
- سياسة الاستخدام الأخلاقي للذكاء الاصطناعي
- سياسة الاحتفاظ بالبيانات والتخلص منها