

السياسة الوطنية لحوكمة البيانات الحكومية



الهيئة العامة للمعلومات
GENERAL INFORMATION AUTHORITY

النسخة 1.1

ديسمبر 2022م

ملخص الوثيقة

الاسم:	السياسة الوطنية لحوكمة البيانات الحكومية.
الإصدار:	1.1، ديسمبر 2022.
نوع الوثيقة:	سياسات.
الملخص:	تهدف الوثيقة إلى إنشاء سياسة عامة تختص بحوكمة البيانات الحكومية، لتشمل كامل دورة حياة البيانات بداية من إنشائها، وتخزينها وتأمينها، وتصنيفها، ومشاركتها، وأرشفتها، ثم تدميرها، على مستوى الحكومة والجهات التابعة لها، مع الالتزام بالمبادئ والقيم الأخلاقية في هذا المجال، بهدف توحيد ومشاركة هذه البيانات، للاستفادة منها في إطلاق الخدمات، ودعم صانعي القرار.
المالك:	الهيئة العامة للمعلومات.

فريق الإعداد

م. يوسف عبدالرحمن أبوراوي

م. عبدالباسط سالم الباعور

مراجعة وتدقيق

د. يحي أحمد الفساطوي

د. عبدالرؤوف علي البياص

تصميم وإخراج

م. سمير معروف

جدول المحتويات

1. مقدمة:	4
2. الغاية والأهداف:	4
3. نطاق السياسة:	5
4. المبادئ والقيم الحاكمة:	5
1.4 الشفافية:	5
2.4 الملكية الفكرية:	5
3.4 خصوصية البيانات:	5
4.4 التكامل:	6
5.4 تحديد المسؤوليات:	6
6.4 الكفاءة الفنية والتشغيلية:	6
7.4 الجودة:	6
5. دورة حياة البيانات:	6
1.5 إنشاء البيانات:	7
2.5 تخزين البيانات وتأمينها:	8
3.5 تصنيف البيانات:	8
1.3.5 معايير تصنيف البيانات:	10
2.3.5 خطوات تصنيف البيانات:	11
4.5 مشاركة البيانات:	13
1.4.5 مبادئ مشاركة البيانات:	13
2.4.5 خطوات مشاركة البيانات:	14
5.5 أرشفة البيانات:	14
6.5 تدمير البيانات:	15
6. ملكية البيانات:	15
7. حماية البيانات:	16

1. مقدمة:

في عالم اليوم، تعتبر البيانات رأس مال واعد، ومورد استراتيجي مهم، حيث تنطوي على إمكانيات هائلة للاستثمار في كل القطاعات، لتقديم العديد من الخدمات وتنظيم وتطوير الأعمال بمختلف أنواعها للوصول إلى مجتمع المعرفة الذي يتيح لأفراده امتلاك البيانات والمعلومات، ونقلها، وبثها، وتبادلها، وتوظيفها، عن طريق التقنيات الحاسوبية، والمعلوماتية، وفق سياسات وتشريعات واضحة ومنظمة، ليكون هدفها النهائي هو تحسين حياة الانسان وزيادة رفاهيته.

وحيث أن البيانات هي المادة الخام للمعلومات وكل ما يترتب عليها من خدمات تهدف إلى إيصال المعرفة للمستفيدين ليتخذوا من خلالها قرارات حكيمة مبنية على حقائق موثقة ومضبوطة، لا مجرد تخمينات أو انطباعات لم تعد مقبولة في عالم يعتبر الدقة مؤشرا واضحا على الجودة.

كل ذلك كان دافعا للهيئة العامة للمعلومات، لإعداد السياسة الوطنية لحوكمة البيانات الحكومية وتعميمها.

2. الغاية والأهداف:

إن الغاية من انشاء هذه السياسة هي تحديد الإطار العام لحوكمة البيانات الحكومية، وتوفير برنامج عمل لتصنيف وإدارة وتبادل هذه البيانات، بما يساهم في تحسين قدرة الجهات الحكومية على التعامل مع البيانات بشكل جيد في كل مراحل دورة حياة البيانات بداية من جمعها وإنتاجها، وصولا إلى حفظها وأرشفتها، لخلق بيئة معلوماتية متكاملة هدفها تقديم خدمات ذات جودة عالية للمواطن، ودعم متخذي القرار في مختلف القطاعات الحكومية.

تهدف السياسة الوطنية لحوكمة لبيانات الحكومية إلى:

- 1- وضع قواعد عامة للتعامل مع البيانات الحكومية في مختلف مراحل دورة حياتها.
- 2- توحيد مفاهيم ومبادئ حوكمة البيانات بين مختلف الجهات الحكومية.
- 3- توحيد إجراءات التعامل مع البيانات.
- 4- نشر الثقافة التقنية وتبنيها للاستفادة المثلى من البيانات.

كما سيتم شرح هذه القواعد والمفاهيم والإجراءات بشكل أكثر تفصيلا في (الدليل الاسترشادي للبيانات)، مع أمثلة للممارسات الأكثر نجاحا في هذا المجال.

3. نطاق السياسة:

- تم وضع هذه السياسة لتكون إطاراً عاماً، لحوكمة البيانات الحكومية، ليتم تطبيقها على:
- 1- كافة الجهات الحكومية بمختلف أنواعها وتبعياتها، التي تنتج البيانات والمعلومات أو تجمعها أو ترسلها أو تشاركها أو تخزنها أو تعالجها.
 - 2- كافة أشكال البيانات، سواء كانت إلكترونية مهيكلية أو غير مهيكلية، أو مطبوعة مؤرشفة أو غير مؤرشفة، سواء تم إنتاجها وتجميعها داخل الجهة الحكومية، أو تم نقلها أو الحصول عليها من خارج هذه الجهة.

4. المبادئ والقيم الحاكمة:

تستند السياسة الوطنية لحوكمة البيانات الحكومية إلى عدد من المبادئ والقيم الحاكمة للتعامل مع البيانات الحكومية، استناداً إلى أفضل الممارسات والتجارب، وهي:

1.4 الشفافية:

الشفافية في تبادل البيانات والمعلومات مبدأ مهم وجوهري لأي سياسة شاملة لحوكمة البيانات، فيجب ألا ينظر إلى البيانات التي تم جمعها أو إنتاجها من قبل أحد الجهات بأنها ملك لتلك الجهة وحدها، بل يجب أن تكون متاحة للتداول مع جهات أخرى وفق حدود الخصوصية والاعتبارات الأمنية والقانونية المنظمة لهذه العملية.

2.4 الملكية الفكرية:

الملكية الفكرية حق أصيل لأصحابها يجب عدم انتهاكه حتى مع وجود مبدأ الشفافية ومشاركة البيانات، بل لابد من وضع تشريعات تنظم وتحفظ حقوق الأفراد والمؤسسات في إنتاجهم الإبداعي.

3.4 خصوصية البيانات:

قبل مشاركة البيانات والمعلومات، يجب النظر في خصوصية البيانات مسبقاً، بحيث يجب أخذ موافقة مالكي هذه البيانات وتصنيفها إلى المستوى المناسب قبل مشاركتها واستخدامها.

4.4 التكامل:

تسعى الحكومة ومختلف جهاتها إلى بناء نظام موحد للربط الشبكي، بهدف تبادل البيانات فيما بينها، وتسهيل عملية الولوج واستخدام البيانات والمعلومات التابعة لها وفق السياسات المحددة، لذلك تتحمل كافة الجهات الحكومية مسؤوليتها لتمكين وتعزيز مشاركة البيانات فيما بينها ووضع الاستراتيجيات والخطط والآليات لتسهيل هذه العملية والمشاركة فيها بفعالية.

5.4 تحديد المسؤوليات:

من المهم معرفة أن اكتمال البيانات وصحتها أمر مهم للغاية، فقد تؤدي البيانات والمعلومات غير الدقيقة إلى آثار كارثية، لذلك يجب أن يتخذ مزودو البيانات والمعلومات جميع الخطوات اللازمة للحفاظ على سلامة بياناتهم، وتحديد المسؤوليات والواجبات بشكل دقيق داخل فرق العمل، ومراقبة الأداء العام وتحديد مكامن الضعف وسوء التنفيذ ومعالجتها.

6.4 الكفاءة الفنية والتشغيلية:

على جميع الجهات الحكومية استخدام التقنيات والمبادئ المثل لضمان التعامل مع البيانات بشكل سلس، واستحداث آليات فعالة من الناحية الفنية والتشغيلية، بحيث تضمن جودة وسلامة بياناتها التي تشاركها، لتكون قيمة مضافة يمكن الاستفادة منها باحترافية، وبأقل جهد بشري.

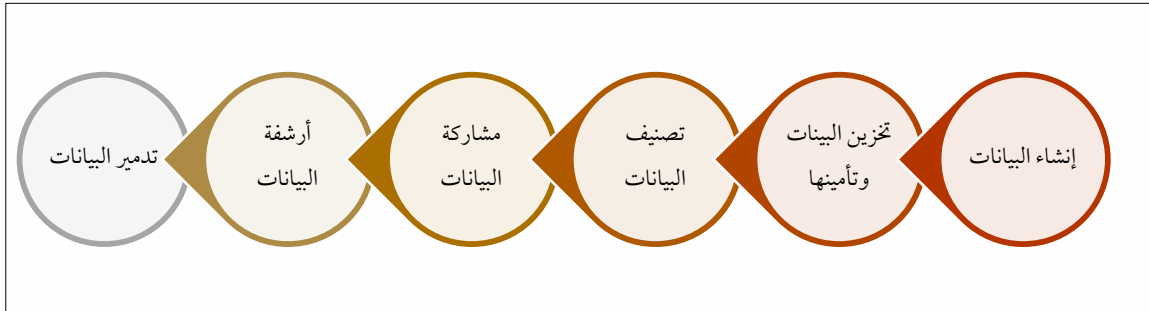
7.4 الجودة:

إن النتيجة النهائية للالتزام بالمبادئ والقيم المذكورة أعلاه في كل مراحل دورة حياة البيانات، هو ضمان جودة وسلامة وتكامل ومصادقية هذه البيانات، لنتمكن من توظيفها لتقديم الخدمات، ودعم متخذي القرار، بكل ثقة وفعالية.

5. دورة حياة البيانات:

دورة حياة البيانات هي المراحل المختلفة التي تمر بها البيانات خلال رحلة تعاملنا معها، من الإنشاء الأولي إلى التدمير، يمكن أحيانا دمج بعض هذه المراحل، أو تفصيل بعضها الآخر حسب الحاجة، ولكن الهدف النهائي لهذا

التقسيم هو الفهم الجيد للمراحل التي تمر بها البيانات، وكيفية التعامل معها في كل مرحلة، السياسة الوطنية لحوكمة البيانات الوطنية اعتمدت المراحل التالية كدورة حياة للبيانات داخل المؤسسات والجهات الحكومية:



الشكل (1) دورة حياة البيانات

1.5 إنشاء البيانات:

المرحلة الأولى من دورة حياة البيانات هي إنشاء البيانات، يمكن أن تكون هذه البيانات بأشكال متعددة المستندات النصية أو الصور أو قواعد البيانات، عادةً ما يتم إنشاء البيانات بواسطة واحدة من الطرق الآتية:

- **تجميع البيانات:** وهو الحصول على البيانات الموجودة بالفعل، والتي تم إنتاجها خارج المؤسسة.
- **التقاط البيانات:** التقاط البيانات التي تم إنشاؤها بواسطة العمليات المختلفة داخل المؤسسة.
- **إدخال البيانات:** وهو الإدخال اليدوي للبيانات الجديدة من قبل الموظفين داخل المؤسسة.

في هذه المرحلة يجب على المؤسسات والجهات الحكومية التأكد من النقاط التالية:

- جميع البيانات والمعلومات والسجلات مخزنة إلكترونياً في أنظمتها، ومؤمنة تأميناً جيداً، وفق القوانين واللوائح والسياسات ذات الصلة.
- التأكد من أن عملية تجميع والتقاط وإدخال البيانات تتم بالطرق المشروعة.
- أن تقتصر عملية تجميع البيانات في المؤسسة على البيانات الضرورية لتلبية متطلباتها وخدماتها والمقتصرة على نشاط عملها.
- يجب على الجهات التأكد من أن جمع المعلومات الشخصية لا يتم إلا بموافقة الشخص المعني على الإفصاح عن هذه البيانات والسماح باستخدامها ومشاركتها.
- يجب على الجهات مراجعة نماذج بياناتها، وتقليصها لأدنى حد ممكن، تنظيمها لهذه البيانات وتقليلاً للازدواجية والتكرار.

2.5 تخزين البيانات وتأمينها:

بمجرد إنشاء البيانات داخل المنظمة، يجب تخزينها وحمايتها، مع تطبيق المستوى المناسب من الأمان الذي تفصله خطط أمن البيانات والأنظمة المعتمدة، كما يجب أن تشمل خطط تخزين البيانات تنفيذ عمليات النسخ الاحتياطي والاسترجاع، لضمان الاحتفاظ الآمن بالبيانات خلال دورة حياتها.

3.5 تصنيف البيانات:

تصنف هذه السياسة البيانات الحكومية، اعتماداً على مدى إمكانية الوصول إليها والاستفادة منها إلى فئتين، الأولى غير متاحة، والثانية متاحة، كما يتم تقسيم هذه الفئات إلى مستويات تصنيف وفق الآتي:

الجدول (1) فئات تصنيف البيانات الحكومية

الفئة	مستويات التصنيف	رقم المستوى
بيانات غير متاحة	سري للغاية	1
	سري	2
	مقيد	3
بيانات متاحة	متاحة لأصحاب المصلحة	4
	متاحة للعامة	5

الجدول (2) مستويات تصنيف البيانات الحكومية

مستوى التصنيف	درجة التأثير	الوصف	أمثلة توضيحية
سري للغاية	عالي	تصنف البيانات بأنها (سرية للغاية)، إذا كان الوصول غير المصرح لها يؤدي إلى ضرر جسيم ولا يمكن تداركه أو إصلاحه على: - المصلحة الوطنية العليا بما فيها سمعة البلد أو علاقاته الدبلوماسية والدولية. - صحة وسلامة الأفراد، والمجتمع. - الأمور الاستخباراتية والأمنية والعسكرية. - الاقتصاد الوطني، والموارد الطبيعية. - البنية التحتية في مختلف المجالات. - الكفاءة التشغيلية وأداء الحكومة والمؤسسات العامة.	- المعلومات المتعلقة بالاتفاقيات أو المعاهدات الدولية السياسية أو الاقتصادية. - أي تحركات أو تجهيزات استخباراتية أو أمنية أو عسكرية. - ما يتعلق بمستويات ومفاتيح التشفير والحماية الإلكترونية الوطنية. - معلومات عن التهديدات بالهجمات الجراثومية أو تسميم المياه والغذاء أو تدمير مواردها. - معلومات عن انتهاكات تؤدي إلى ضرر جسيم بالاقتصاد الوطني أو البيئة والمواد الطبيعية بكل أنواعها.

- مذكرات التفاهم الدولية الخاصة بالجانب الاقتصادي. - معلومات عن الامدادات اللوجستية والأمن الغذائي والمائي. - معلومات عن المنشآت الحيوية ومحتوياتها.	تصنف البيانات بأنها <u>سرية</u>، إذا كان الوصول غير المصرح لها يؤدي إلى ضرر جسيم ولكن بشكل أقل تأثيراً أو انتشاراً من المستوى السابق، مثل: - ضرر جزئي بالمصلحة الوطنية العليا، بما فيها سمعة البلد أو علاقاته الدبلوماسية والدولية. - أذى أو إصابة مجموعة من الأفراد. - تضرر الاقتصاد الوطني أو الموارد الطبيعية. - ضرر جزئي للبنية التحتية، أو القدرة على تشغيلها وصيانتها. - عرقلة أداء الحكومة والمؤسسات العامة.	متوسط	سري
- معلومات تضر بسمعة أي شخصية (عامة - عادية - اعتبارية). - المعلومات الشخصية (مثل: الرقم الوطني - رقم الهاتف - أرقام الحسابات البنكية)، والمعلومات الصحية للأفراد. - المعلومات المتعلقة بالبحوث والدراسات وتطوير المنتجات، قبل نشرها. - سياسات وإجراءات ورسائل ومذكرات وقوائم البريد الإلكتروني، للمؤسسات والجهات المختلفة، المتعلقة بعملها الداخلي.	تصنف البيانات بأنها <u>مقيدة</u>، إذا كان الوصول غير المصرح لها يؤدي إلى: - ضرر محدود على سير العمل أو الأنشطة الاقتصادية للمؤسسات العامة أو الخاصة أو الأفراد. - ضرر محدود على أصول المؤسسات أو الموارد الطبيعية.	منخفض	مقيد
كل ما يتم مشاركته بين الجهات المختلفة لإتمام أي إجراءات أو لتقديم أي خدمات، وتكون الاستفادة منه داخليا فقط كمحاضر الاجتماعات، المذكرات الداخلية، المعلومات المتعلقة بالمواطنين، وغيرها.	تصنف البيانات بأنها <u>متاحة لأصحاب المصلحة</u>، إذا كان الوصول غير المصرح لها لا يؤدي إلى أي من المخاطر المذكورة أعلاه، أي أنها لا تلحق أي ضرر بالبلد وعلاقاته الدولية، ولا بالأفراد بمختلف أنواعهم، ولا بالاقتصاد والمواد الطبيعية، ولا تنتهك أي مستوى من مستويات التصنيف السابقة. يكون تداول هذه البيانات متاحاً فقط لفئة محددة من الأفراد أو الجهات يعرفون بأصحاب العلاقة، وهم الذين يقتضي عملهم الاطلاع على هذه المعلومات ومعالجتها، ولا يجوز افشاءها أو نشرها خارج نطاق أصحاب العلاقة	لا يوجد في حدود أصحاب المصلحة	متاح لأصحاب المصلحة

- كل ما يتم نشره من الجهات والمؤسسات الحكومية بصورة رسمية، والذي يشمل: - المعلومات - الإجراءات - الإحصاءات - الإعلانات - المنتجات - الخدمات - التقارير - المواقع الإلكترونية وعناوين البريد الإلكتروني والهواتف. - مؤشرات الأداء الرئيسية (KPIs) للجهات والمؤسسات الحكومية.	تصنف البيانات بأنها (متاحة للعامة / مفتوحة)، إذا كان الوصول غير المصرح لمحتواها لا يؤدي إلى أي من المخاطر المذكورة أعلاه، ويمكن إتاحتها للجميع لأنها لا تلحق الضرر بأحد، بل غالباً تكون مفيدة ونافعة للجمهور.	لا يوجد	متاح للعامة (البيانات المفتوحة)
---	--	----------------	---

1.3.5 معايير تصنيف البيانات:

بناء على مستويات التصنيف المذكورة في الجدول (2)، تقوم الجهات بتصنيف بياناتها حسب درجة أهميتها وحساسيتها وتأثيرها، وفي حال وجود بيانات غير مصنفة تعامل على أساس أنها (مقيدة)، حتى يتم تصنيفها بالشكل الصحيح، مع التوجيه بضرورة تصنيف البيانات أولاً بأول، ووضع خطط مضبوطة زمنياً لتصنيف البيانات القديمة.

إن احتمال تصنيف البيانات يتيح للمؤسسة إمكانية حوكمة هذه البيانات بطريقة واعية تعكس قيمتها وتزيد من قيمة ما يمكن استخلاصه منها، بدلاً من التعامل مع جميع البيانات بنفس الطريقة مما يضيع كثيراً من فوائدها الكامنة.

يمكن اختيار تصنيف البيانات بالاعتماد على معايير مختلفة، من أمثلتها:

• التصنيف على أساس المحتوى:

يستخدم لتصنيف البيانات استناداً إلى محتواها، مثلاً يتم تقسيم الوثائق أو رسائل البريد الإلكتروني إلى: عامة، وداخلية، وخارجية، أو أي تقسم آخر يتناسب مع طبيعة عمل الجهة، قد تتطلب هذه العملية مراجعة كل الوثائق أو الرسائل، مما يستغرق وقتاً طويلاً، كما يمكن أتمتها باستخدام البحث عن الكلمة الأساسية في هذه الوثائق، بعد ذلك يتم ربط كل قسم بمستوى من مستويات تصنيف البيانات المناسب له.

• التصنيف على أساس الوصول:

لاستخدام هذا المعيار يتم تقسيم البيانات حسب نوع الأشخاص أو الجهات القادرة على الوصول إلى هذه البيانات أو الوثائق، ثم ربط كل مجموعة من الوثائق أو البيانات بمستوى التصنيف المناسب لها، مثلاً الوثائق التي لا يمكن الوصول إليها إلا من القيادة العليا تصنف بأنها (سرية للغاية)، وهكذا.

• التصنيف على أساس موقع البيانات:

حيث يصنف هذا المعيار البيانات أو الوثائق استناداً إلى مكانها الجغرافي أو مواقع تخزينها على الشبكة، مثلاً ربما تكون العقود المهمة الخاصة بالمؤسسة في مجلد واحد على خادم الملفات، يمكن عندها تطبيق أحد مستويات التصنيف (سري للغاية أو سري) على هذا المجلد ليطبق تلقائياً على جميع مستندات هذا المجلد.

• التصنيف القائم على السياق:

باستخدام هذا المعيار يتم تقسيم البيانات اعتماداً على السياق أو الخصائص المرتبطة بإنشاء وإدارة البيانات، مثل:

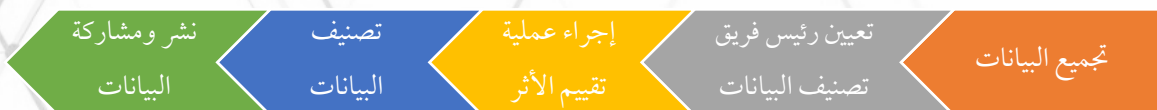
- التطبيق الذي أنشأ الملف، مثل البرامج المالية.
 - الشخص الذي قام بإنشاء المستند، مثل المدير أو مدخل البيانات.
 - الموقع الذي تم فيه إنشاء الملف، أو تعديله، مثل مبنى قسم التسويق.
- ثم يتم ربط كل قسم بمستوى التصنيف المناسب له.

لا توجد قواعد ثابتة للتصنيف، فهو يعتمد بشكل كبير على عدد من العوامل التي تتغير من وقت لآخر حسب الظروف والمستجدات، ويمكن دمج أكثر من معيار أو استحداث معايير جديدة بالخصوص. المهم أن تحدد كل جهة معايير وآليات تصنيفها بشكل واضح، لا يحدث خلطاً في مستويات تصنيف البيانات لديها.

2.3.5 خطوات تصنيف البيانات:

لتم عملية تصنيف البيانات داخل المؤسسة بشكل علمي وعملي، يجب ان تكون هذه العملية مضبوطة وموحدة بين جميع الجهات، وفق خطوات واضحة تتمثل في التالي:

- 1- تجميع البيانات: في هذه الخطوة يتم حصر وجرد كافة البيانات التي تمتلكها الجهة.
- 2- تعيين رئيس فريق حوكمة البيانات: وهو شخص يقوم بقيادة فريق حوكمة البيانات داخل المؤسسة، ويتحمل كامل مسؤولية هذا العمل، ويجب أن يفهم بشكل جيد طبيعة البيانات في المؤسسة وقيمتها، كما يجب أن يكون مطلعاً على استراتيجيات وأهداف وطبيعة عمل المؤسسة، وعليه اختيار فريق العمل القادر على إنجاز المهمة، وتقسيم الأدوار والمهام داخل فريق العمل، لإتمام عملية التصنيف بالشكل المطلوب.
- 3- إجراء عملية تقييم الأثر: يجب على فريق تصنيف البيانات البدء في تقييم أثر تصنيف كل مجموعة من البيانات المدروسة، وذلك بدراسة مدى تأثير هذا التصنيف وما يترتب عليه من عواقب للوصول إلى مستوى التصنيف المناسب لهذه البيانات، نقترح الآلية التالية لدراسة تقييم الأثر:
 - افتراض أن البيانات (سرية للغاية) للمؤسسات السياسية والأمنية، ثم دراسة حساسية وطبيعة البيانات، وإمكانية تصنيفها إلى مستويات أدنى.
 - افتراض أن البيانات (متاحة للعامة/ مفتوحة) لباقي المؤسسات والجهات، ثم دراسة حساسية وطبيعة البيانات، وإمكانية تصنيفها إلى مستويات أعلى.
 - في كلا الحالتين على فريق التصنيف الموازنة بين مزايا ومساوئ الإفصاح عن البيانات من عدمه، ورصد ما يترتب على كل مستوى من مستويات التصنيف، وارتباط هذه البيانات بغيرها من الأنظمة والمؤسسات، للوصول إلى المستوى المناسب من التصنيف.
- 4- تصنيف البيانات: بعد التأكد من صلاحية مستوى التصنيف للبيانات المدروسة، يتم تطبيق التصنيف عليها بشكل رسمي.
- 5- نشر ومشاركة البيانات: بعد إتمام عملية التصنيف رسمياً، يمكن للجهة مشاركة هذه البيانات مع الجهات الأخرى (بيانات متاحة لأصحاب المصلحة)، أو إتاحتها ونشرها للعامة (بيانات متاحة للعامة/ مفتوحة).



الشكل (2) خطوات تصنيف البيانات

4.5 مشاركة البيانات:

تشمل هذه السياسة كل الجهات الحكومية، فبعد أن تكمل كل مؤسسة عملية تصنيف البيانات المستهدفة لديها وتجهزها للنشر، يصبح من الممكن تبادل هذه البيانات داخل نطاق المؤسسة نفسها، أو خارجيا بين الجهات المختلفة، بل إن هذا التبادل للبيانات هو هدف أساسي للحكومة لما يشكله من قيمة مضافة واستفادة مباشرة من كمية البيانات المنتجة داخل مؤسساتها.

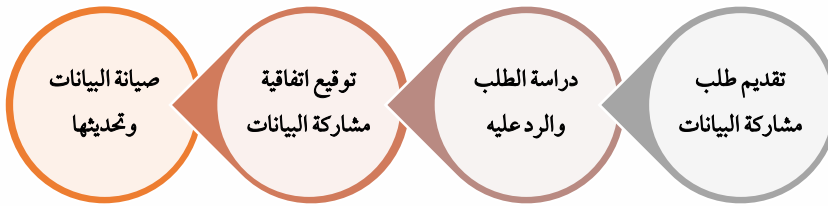
تهدف عملية تبادل ومشاركة البيانات للوصول إلى مبدأ إدخال أو توليد البيانات لمرة واحدة، ثم الاستفادة منها في كل القطاعات والجهات الأخرى، توفيراً للوقت والجهد والموارد، والاستفادة المثلى من البيانات.

1.4.5 مبادئ مشاركة البيانات:

- 1- **مشروعية الهدف:** يجب أن تكون عملية تبادل البيانات لهدف مشروع أو حاجة حقيقية لتحقيق مصلحة عامة أو تقديم خدمة، دون الاضرار بالأفراد أو المؤسسات أو المصلحة الوطنية، وضمن إطار واضح ومقتن.
- 2- **التصريح بالوصول:** يجب أن تمتلك الجهات التي تتبادل البيانات صلاحية الاطلاع على البيانات واستخدامها.
- 3- **الكفاءة الفنية:** يجب أن تمتلك الجهات التي تتبادل البيانات، فريقاً لحوكمة البيانات، مكوناً من الأشخاص المؤهلين المسلحين بالمعارف والمهارات اللازمة للتعامل مع البيانات.
- 4- **الشفافية:** يجب على جميع الجهات التي تتبادل البيانات إتاحة جميع المعلومات المتعلقة بالبيانات المتبادلة، وطريقة التعامل معها بالصورة المثلى كوسائل نقلها وطرق حفظها ومعالجتها.
- 5- **المسؤولية المشتركة:** يجب التنسيق بين الجهات التي تتبادل البيانات لأن المسؤولية ستكون مشتركة بينها في تطبيق جميع الضوابط والاتفاقيات والتشريعات المنظمة لتبادل البيانات وتأمينها.
- 6- **الاستخدام الأخلاقي:** يجب الالتزام بتطبيق الممارسات الأخلاقية أثناء عملية تبادل البيانات ومشاركتها للوصول إلى العدالة والنزاهة والأمانة المهنية.

2.4.5 خطوات مشاركة البيانات:

- 1- تتقدم الجهة المستوردة للبيانات بطلب رسمي للجهة المصدرة للبيانات.
- 2- يتم تحويل الطلب إلى فريق حوكمة البيانات في الجهة المصدرة للبيانات، ليقوم بدراسة الطلب والتأكد من استيفاء جميع مبادئ مشاركة البيانات، وتحديد مستوى تصنيف البيانات المطلوبة، والرد بالموافقة أو الرفض.
- 3- في حال الموافقة يجب توقيع اتفاقية مشاركة البيانات بين الجهتين المصدرة والمستوردة، وإتمام عملية مشاركة البيانات.
- 4- تلتزم الجهة المصدرة للبيانات بوضع التدابير اللازمة لصيانة البيانات بما في ذلك أي تحديثات لاحقة للبيانات وإعادة مشاركتها مع الجهات المستوردة للبيانات.



الشكل (3) خطوات مشاركة البيانات

5.5 أرشفة البيانات:

أرشفة البيانات هي عملية تتم على البيانات التي أصبحت غير نشطة إما لتقادم هذه البيانات أو لطبيعتها الخاصة، وتتم عملية الأرشفة بنسخ البيانات في مستودعات تخزين خاصة بها، وإزالتها من بيئة التشغيل النشطة، مع إمكانية استعادة هذه البيانات إلى البيئة النشطة واستخدامها عند الحاجة إليها، في هذا الجانب يجب على المؤسسات الحكومية الالتزام بالتالي:

- إنشاء سياسة أرشفة تتناسب مع سياساتها وطبيعتها استخدامها للبيانات.
- إجراء عمليات الأرشفة للبيانات بصورة دورية.
- تأمين المخازن والخوادم الخاصة بالأرشفة بنفس مستويات الحماية والتأمين للأنظمة والبيانات النشطة.

6.5 تدمير البيانات:

ينمو حجم البيانات المؤرشفة باستمرار، لذلك فإنه من غير الممكن الاستمرار في الاحتفاظ بالبيانات إلى الأبد، فتكاليف التشغيل التخزين والأرشفة تتزايد أيضا، كما أن كثير من البيانات المخزنة تفقد أهميتها تماما بمرور الزمن، لذلك يجب أن تبين التشريعات المدة الزمنية التي يجب الاحتفاظ فيها ببيانات المؤسسة، والتي يمكن بعدها إتلاف هذه البيانات وتدميرها بدون أي ضرر.

عادة ما تتم عملية تدمير البيانات في مستودعات الأرشفة، بعد تجاوزها فترة الاحتفاظ القانونية، والتأكد تماما من عدم حاجتنا إليها مستقبلا.

6. ملكية البيانات:

كل البيانات التي تجمعها أو تنتجها أي جهة أو مؤسسة حكومية، هي في النهاية ملك للحكومة الليبية، لذا يجب أن تكون متاحة للتداول والمشاركة مع الجهات الأخرى التي يقتضي عملها ذلك، في حدود القوانين والسياسات والتشريعات النافذة.

لذلك قبل البدء في جمع أي بيانات جديدة من أي جهة، يجب الاستعلام عن وجود هذه البيانات من الجهات التي يمكن أن تكون قد جمعتها من قبل، تجنبنا لإعادة تجميعها أو انتاجها، وتوفيرا للجهود والأموال التي ستهدر نتيجة تكرار عملية التجميع، وتحقيق مبدأ إدخال أو توليد البيانات لمرة واحدة، وتعزيز سياسة إعادة الاستخدام.

وملحق مع هذه السياسة دليل مرجعي للبيانات على المستوى الوطني، للوصول إلى أقصى استفادة من البيانات المجمعة والمنتجة والمصنفة في الجهات التابعة لها.

7. حماية البيانات

حماية البيانات هي عملية ترافق البيانات في كامل دورة حياتها، وهي من أكثر العمليات حساسية ودقة عند التعامل مع البيانات، كما أن مستويات الحماية والتأمين متعددة، تشمل أمن البيانات، وأمن الأنظمة، وأمن الشبكات، لذلك يجب على كل مؤسسة الالتزام بالتالي:

- يجب على الجهات والمؤسسات تطوير سياسات أمنية تحمي ما تمتلكه من بيانات وأنظمة، بحيث تضمن هذه السياسات عدم الوصول أو المشاركة أو التعديل غير المصرح به، وبما يتوافق مع القوانين واللوائح النافذة.
- على الجهات مراجعة سياساتها بصورة دورية تضمن وجود احتياطات كافية لحماية البيانات، ومعالجة أي ثغرات مكتشفة في أنظمة وسياسات الحماية لديها.
- يجب على الجهات التأكد من وجود إجراءات أمنية تضمن سلامة وسرية البيانات التي يتم الحصول عليها من جهات أخرى، وعدم السماح بإفشائها.
- الاهتمام بتأمين الشبكات ووسائل النقل ومعدات التشبيك، لوجود كثير من الاختراقات الأمنية التي تتم في هذا المستوى.
- يجب حماية الموقع الإلكتروني للمؤسسة، وكل البيانات الموجودة عليه أو المجمعة من خلاله، بما يتفق مع السياسات الأمنية المعلن عنها.
- انشاء خطط النسخ الاحتياطي للبيانات، وتوفير مراكز بيانات بديلة، تحسباً لأي طارئ أو كارثة محتملة.

تم اعداد الوثيقة بالهيئة العامة للمعلومات	
النسخة:	1.1 ، ديسمبر 2022
الموقع الإلكتروني:	https://gia.gov.ly/
البريد الإلكتروني:	info@gia.gov.ly