

السياسة الوطنية لحكومة البيانات الحكومية

الهيئة العامة للمعلومات
GENERAL INFORMATION AUTHORITY
STATE OF LIBYA
دولة ليبيا



النسخة الأولى
أبريل 2025 م

السياسة الوطنية لحكومة البيانات الحكومية

الهيئة العامة للمعلومات
GENERAL INFORMATION AUTHORITY
STATE OF LIBYA
دولة ليبيا

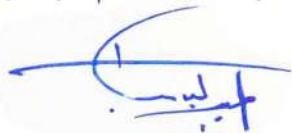




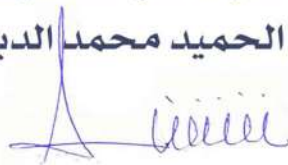
WWW.FREEPIK.COM

مصدر صورة الفلايق
www.freepik.com

رئيس الهيئة العامة للمعلومات
م. عبد الباسط سالم الباعور



رئيس حكومة الوحدة الوطنية
م. عبد الحميد محمد الدبيبة



أبريل 2025

ملخص الوثيقة

الاسم:	السياسة الوطنية لحكومة
الإصدار:	1.1 أبريل 2025.
نوع الوثيقة:	سياسات
الملخص:	تهدف الوثيقة إلى إنشاء سياسة عامة تختص بحكومة البيانات الحكومية، لتشمل كامل دورة حياة البيانات بداية من إنشائها وتخزينها وتأمينها ومشاركتها وأرشفتها، حتى أتلافها 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 أبو راوي

م. عبدالباسط سالم الباعور

مراجعة وتدقيق

د. يحيى أحمد الفساطوي

د. عبدالرؤف علي البيباص

تصميم وإخراج

م. سمير محمد معروف

جدول المحتويات

8	1. مقدمة:
8	2. الغاية والأهداف:
9	3. نطاق السياسة:
9	4. المبادئ والقيم الحاكمة:
9	1.4 الشفافية:
9	2.4 الملكية الفكرية:
9	3.4 خصوصيات البيانات:
10	4.4 التكامل:
10	5.4 تحديد المسؤوليات:
10	6.4 الكفاءة الفنية والتشغيلية:
10	7.4 الجودة:
10	5. دورة حياة البيانات:
11	1.5 إنشاء البيانات:
12	2.5 تخزين البيانات وتأمينها:
12	3.5 تصنيف البيانات:
14	1.3.5 معايير تصنيف البيانات:
15	2.3.5 خطوات تصنيف البيانات:
17	4.5 مشاركة البيانات:
17	1.4.5 مبادئ مشاركة البيانات:
18	5.5 تدمير البيانات:
18	6. ملكية البيانات:
19	7. حماية البيانات:

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 الإنسان 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 مقبول في عالم يعتبر الدقة مؤشراً واضحاً على الجودة.

فإن كل ذلك كان دافعاً للهيئة العامة للمعلومات لإعداد السياسة الوطنية لحكومة البيانات الحكومية وتعميمها.

2. الغاية والأهداف:

أن الغاية من إنشاء هذه السياسة هي تحديد الإطار العام لحكومة 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، وصولاً إلى حفظها وأرشفتها لخلق بيئة معلوماتية متكاملة هدفها تقديم خدمات ذات جودة عالية للمواطن، ودعم متخذي القرار في مختلف القطاعات الحكومية.

تهدف السياسة الوطنية لحكومة البيانات الحكومية إلى:

1- وضع قواعد عاملة 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 الثقة التقنية وتبنيها للاستفادة المثلى من البيانات.

وسيتم شرح هذه القواعد والمفاهيم والإجراءات بشكل أكثر تفصيلاً في **(الدليل الاسترشادي للبيانات)** مع أمثلة للممارسات الأكثر نجاحاً في هذا المجال.

3. نطاق السياسة:

- تم وضع هذه السياسة لتكون إطاراً عاماً لحوكمة البيانات ليتم تطبيقها على:
- 1- كافة الجهات الحكومية التي تنتج البيانات والمعلومات أو تجمعها أو ترسلها أو تشاركها أو تخزنها أو تعالجها.
 - 2- كافة أشكال البيانات سواء أكانت إلكترونية مهيكلة أو غير مهيكلة 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 أخذ موافقة مالكي هذه البيانات وتصنيفها إلى المستوى المناسب قبل مشاركتها أو استخدامها.

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 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 المثلى 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 ومصداقية 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 تعاملنا معها، من الإنشاء الأولى إلى التدمير، يمكن أحياناً دمج 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 لحكومة 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 البيانات هي إنشاء البيانات، يمكن أن تكون هذه البيانات بأشكال متعددة كالمستندات النصية أو الصور أو قواعد البيانات، وعادةً ما يتم إنشاء البيانات بواسطة إحدى 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:

- جمع 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، تنظيمياً 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 البيانات تنفيذ عمليات النسخ الاحتياطي والاسترجاع لضمان الاحتفاظ الآمن بالبيانات خلال دورة حياتها.

3.5 تصنيف البيانات:

تصنيف هذه السياسة للبيانات 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

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

الجدول (2) مستويات تصنيف البيانات الحكومية

أمثلة توضيحية	الوصف	درجة التأثير	مستوى التصنيف
<ul style="list-style-type: none"> 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 الجرثومية أو تسميم المياه والغذاء أو تدمير مواردها. معلومات عن انتهاكات تؤدي إلى ضرر جسيم بالاقتصاد الوطني أو البيئة والموارد الطبيعية بكل أنواعها. 	<p>تصنيف البيانات بأنها (سرية للغاية) إذا كان الوصول غير المصرح لها يؤدي على ضرر جسيم ولا يمكن تداركه أو إصلاحه على:</p> <ul style="list-style-type: none"> - المصلحة الوطنية العليا بما فيها سمعة البد 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. 	عالي	سري للغاية
<ul style="list-style-type: none"> مذكرات التفاهم الدولية الخاصة بالجانب الاقتصادي. معلومات عن الإمدادات اللوجستية والأمن الغذائي والمائي. معلومات عن المنشآت الحيوية ومحتوياتها. 	<p>تصنيف البيانات بأنها (سرية) إذا كان الوصول غير المصرح لها يؤدي إلى ضرر جسيم ولكن بشكل أقل تأثيراً أو انتشاراً من المستوى السابق مثل:</p> <ul style="list-style-type: none"> - 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
<ul style="list-style-type: none"> 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 . 	<p>تصنيف البيانات بأنها (مقيدة) إذا كان الوصول غير المصرح لها يؤدي إلى:</p> <ul style="list-style-type: none"> - ضرر محدود على سير العمل أو الأنشطة الاقتصادية للمؤسسات العامة أو الخاصة أو الأفراد. - ضرر محدود على أصول المؤسسات أو الموارد الطبيعية. 	منخفض	مقيد
<ul style="list-style-type: none"> كل ما يتم مشاركته بين الجهات المختلفة لإتمام أي إجراءات أو لتقديم أي خدمات وتكون الاستفادة منه داخلياً فقط كمحاضر 	<p>تصنيف البيانات بأنها (متاحة لأصحاب المصلحة) 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</p>		متاح لأصحاب المصلحة

<p>الاجتماعات، المذكرات الداخلية، المعلومات المتعلقة بالمواطنين وغيرها.</p>	<p>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 إفشاؤها أو نشرها خارج نطاق أصحاب العلاقة.</p>		
<p>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</p>	<p>تصنيف 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.</p>		<p>متاح للعامة (البيانات المفتوحة)</p>

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 اكتمال 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 تقسيم آخر يتناسب مع طبيعة عمل الجهة، وقد 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 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.
- 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:

لتنفيذ عملية تصنيف البيانات داخل المؤسسة بشكل علمي وعملي، يجب أن 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 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 وإمكانية تصنيفها إلى مستويات أعلى.
 - افتراض أن البيانات (متاحة للعامة / مفتوحة) لباقي المؤسسات والجهات، ثم دراسة حساسية وطبيعة البيانات، وإمكانية تصنيفها إلى مستويات أعلى.
 - في كلتا 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 خارجياً بين الجهات المختلفة، بل وإن 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 ومن 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 الأضرار بالأفراد أو المؤسسات أو المصلحة الوطنية، ضمن إطار واضح ومقنن.
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 والمتسلحين 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 فيما 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.

5.5 تدمير البيانات:

ينمو حجم البيانات المؤرشفة باستمرار، لذلك فإنه من غير الممكن الاستمرار في الاحتفاظ بالبيانات إلى الأبد، فتكاليف التشغيل والتخزين والأرشفة تتزايد أيضاً، كما أن كثير من البيانات المخزنة تفقد أهميتها تماماً 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 الإحتفاظ القانونية، والتأكد تماماً من عدم حاجتنا إليها مستقبلاً.

6. ملكية البيانات:

كل البيانات التي تجمعها أو تنتجها أي جهة مؤسسة حكومية، هي في النهاية ملك للحكومة اللببية، 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، تجنباً لإعادة تجميعها أو إنتاجها، وتوفيراً للجهود والأموال التي ستهدر نتيجة تكرار عملية التجميع، وتحقيق مبدأ إدخال أو توليد البيانات لمرة واحدة، وتعزيز سياسة إعادة الاستخدام.

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

7. حماية البيانات:

- حماية البيانات هي عملية ترافق البيانات في كل 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.
 - إنشاء خطط الاحتياطي للبيانات، وتوفير مراكز بيانات بديلة، تحسباً لأي طارئ أو كارثة محتملة.

تم إعداد الوثيقة بالهيئة العامة للمعلومات	
1.1 أبريل 2025	الإصدار:
https://gia.iy/	الموقع الإلكتروني:
info@gia.gov.ly	البريد الإلكتروني:

