عـــــــــام - Public

مكتب إدارة البيانات

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture

سياسة حماية البيانات الشخصية

الإصدار: 3.3

سبتمبر 2025

معلومات المستند:

اسم المستند	سياسة حماية البيانات الشخصية
تاريخ الإنشاء	1 يناير 2023
تاريخ النفاذ	يناير 2026
تاريخ النشر	يناير 2026
تصنيف المستند	عام
مؤلف المستند الأصلي	فريق مكتب إدارة البيانات

معلومات الإصدار الحالي:

رقم الإصدار	3.3		
من إعداد	فريق مكتب إدارة البيانات	التاريخ	سبتمبر 2025
المراجعة من قبل	الإدارة العامة للأمن السيبراني	التاريخ	سبتمبر 2025
التحديث النهائي	فريق مكتب إدارة البيانات	التاريخ	سبتمبر 2025
تم الاعتماد من قبل	اللجنة التنفيذية لإدارة وحوكمة البيانات	التاريخ	يناير 2026
	اللجنة العليا للتحول الرقمي	التاريخ	أبريل 2023
مالك المستند	مكتب إدارة البيانات		

قائمة الإصدارات:

رقم الإصدار	إعداد	التاريخ	التعديل
V3.3	مكتب إدارة البيانات	07 سبتمبر 2025	بعد مراجعة فريق مكتب إدارة البيانات بمركز وقاء لسياسات المكتب تم: 1. تعديل ضوابط خصوصية البيانات حسب الضوابط الصادرة من سدايا. 2. تعديل المسمى الوظيفي ل "أمين البيانات" ب"فريق الدعم الفني والتقني"
V2.0	مكتب إدارة البيانات	20 مايو 2024	1. بعد مراجعة السياسة من طرف فريق سدايا خلال الزيارة الميدانية لمكتب إدارة البيانات بالوزارة بتاريخ 19 مايو 2024، تم تعديل السياسة لتشمل: 2. إضافة جميع عمليات تصنيف البيانات وتوصيفها للسياسة 3. إضافة دورية مراجعة تصنيف البيانات حسب نوع التصنيف
V1.0	مكتب إدارة البيانات	1 مارس 2023	النسخة المبدئية
V0.1	مكتب إدارة البيانات	14 يناير 2022	مسودة أولية

بسم الله الرحمن الرحيم

فهرس المحتويات

1. مقدمة

تسعى المملكة لتطبيق أفضل الممارسات العالمية لسياسات وضوابط إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية وتعزيز القيمة المستفادة منها في اتخاذ القرارات الاستراتيجية واستشراف المستقبل وتحقيق أعلى مستويات المسؤولية والشفافية.
ومن هذا المنطلق، قام مكتب إدارة البيانات بالوزارة بإعداد سياسة حماية البيانات الشخصية والتي تتضمن الحقوق والقواعد العامة التي يجب على الجهات المشمولة بنطاق تطبيق هذه السياسة مراعاتها والالتزام بها للحد من الممارسات الخاطئة المتعلقة بمعالجة البيانات الشخصية وضمان حمايته أصحاب البيانات من الآثار السلبية والمخاطر المحتملة، بالإضافة إلى المحافظة على خصوصيتهم وحماية حقوقهم.

1.1. الغرض

إشارة إلى قرار مجلس الوزراء رقم (292) وتاريخ 27/4/1441 هـ القاضي في الفقرة (1) من المادة عاشرا بأن يتولى مكتب البيانات الوطنية وضع السياسات وآليات الحوكمة والمعايير والضوابط الخاصة بالبيانات والذكاء الاصطناعي ومتابعة الالتزام بها بعد إقرارها، عليه فقد قام مكتب إدارة البيانات الوطنية والاستفادة من الممارسات والمعايير العالمية عند إعداد سياسة حماية البيانات والتي تهدف إلى التأكد من أن البيانات تخضع لمستوى مناسب من الحماية وفقًا لمدى أهميتها بالنسبة إلى الوزارة، ويرجع الغرض من حماية البيانات هو وضع القواعد وتقديم إرشادات حول حماية خصوصية المعلومات للأفراد والقطاعات التابعة لوزارة البيئة والمياه والزراعة، وأي معلومات تعريفية، والحفاظ على سرية البيانات الشخصية التي تخص العملاء والموظفين وشركاء الأعمال. كما أنه يضمن الامتثال للوائح القانونية الخاصة بالوزارة.

1.2. مجال العمل

تشمل أحكام هذه السياسة جميع البيانات الشخصية التي تنتجها أو تتلقاها وزارة البيئة والمياه والزراعة، أو أية بيانات شخصية خاصة بالقطاعات التابعة لها، ويشمل ذلك أيضاًبيانات العملاء والموظفين وشركاء الأعمال.
وتطبق سياسة حماية البيانات الشخصية على ما يلي:

- جميع القطاعات ووحدات العمل التابعة للوزارة.
- جميع موظفي الوزارة والمراكز التابعة لها، العاملين في وظائف بدوام كامل أو دوام جزئي، أو ممن تم التعاقد معهم لتنفيذ مهام محددة.
- الجهات الخارجية المتعاقدة أو المشاركة مع الوزارة والتي يتضمن مجال العمل معها التعامل مع بيانات الوزارة والمراكز التابعة لها.

يستثنى من نطاق تطبيق هذه السياسة، جمع البيانات من غير صاحبها مباشرة - دون علمه - أو معالجتها لغير الغرض الذي جُمعت من أجله أو الإفصاح عنها دون موافقته أو نقلها خارج المملكة في الأحوال التالية:

- إذا كانت الجهة حكومية وكان جمع البيانات أو معالجتها مطلوباً لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء مُتطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفاً فيها.
- إذا كان جمع البيانات أو معالجتها ضرورياً لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

ولمزيد من التفاصيل، يرجى الرجوع إلى الجزء الخاص ب "معالجة البيانات الشخصية".

1.3. مالك السياسة

يعدّ مكتب إدارة البيانات بالوزارة المالك لهذه السياسة والمسؤول عن تحديثها ونشرها.

1.4. إدارة الوثيقة

- يعد قسم حوكمة البيانات في مكتب إدارة البيانات المسؤول عن تطوير وتحديث واعتماد هذه السياسات ومتابعتها.
- جميع الوحدات التنظيمية في الوزارة والمراكز التابعة لها مسؤولة عن الالتزام بهذه السياسة وتنفيذها.
- تتوفر سياسة حماية البيانات الشخصية بكل سهولة لجميع موظفي وزارة البيئة والمياه والزراعة. ومن المقرر نشر السياسات والعمليات ذات الصلة في مكتبة سياسات الوزارة.
- تقع مسؤولية التدريب المحدد المتعلق بسياسات حوكمة البيانات على عاتق مكتب إدارة البيانات بالوزارة.

1.5. التعريفات والمصطلحات

1. الوزارة: وزارة البيئة والمياه والزراعة.
2. مكتب إدارة البيانات: يعدّ مكتب إدارة البيانات المالك الرئيسي لهذه السياسة، كما أنه الجهة المسؤولة عن ضمان تنفيذها بما يتماشى مع احتياجات الوزارة.
3. وحدات الأعمال (BUs): وحدات الأعمال التابعة لوزارة البيئة والمياه والزراعة - مثل وكالة الزراعة، ووكالة المياه، ووكالة البيئة.
4. الوحدات الوظيفية(FUs) : يُقصد بها الوحدات الوظيفية بوزارة البيئة والمياه والزراعة، مثل الموارد البشرية والمالية وغيرها.
5. الوصول(Access) : تدفق المعلومات بين أحد مخازن البيانات والمستخدم أو النظام أو العملية. ويُعتبر من حق المستخدم أو النظام أو العملية الوصول إلى البيانات في حالة وجود امتياز واحد أو أكثر من الامتيازات التالية: القدرة على قراءة البيانات أو عرضها أو تحديث البيانات الموجودة، أو إنشاء بيانات جديدة، أو حذف

البيانات، أو القدرة على إنشاء نسخة من البيانات. كما يمكن منح الوصول إما على أساس مستمر، أو لمرة واحدة فقط، أو على أساس مخصص.

6. جمع البيانات(Data Collection) : التجميع المنتظم للبيانات لغرض محدد من مصادر مختلفة، متضمنًا ذلك الإدخال اليدوي في نظام المعلومات، و الاستبيانات، والمقابلات، والملاحظة، والسجلات القائمة، والأجهزة الإلكترونية. ويتضمن ذلك كلاً من مجموعات البيانات التشغيلية ومستودعات البيانات.
7. الاحتفاظ بالبيانات(Data Retention) : عبارة عن الفترة التي يجب خلالها حفظ البيانات وعدم حذفها. ويمكن الاحتفاظ بالبيانات بأي تنسيق وفي أي نظام على النحو المتفق عليه، كما يمكن لجميع المستخدمين المصرح لهم الوصول إليها في سياق العمل العادي.
8. أرشفة البيانات(Data Archiving) : عبارة عن تخزين آمن للبيانات، يتعذّر معه على المستخدمين المصرح لهم الوصول إليها في سياق العمل العادي، إلا أنه يمكن استرجاعها من جانب مسؤول النظام الذي يعيّنه مدير ممثل بيانات الأعمال.
9. إتلاف البيانات(Data Destruction) : أي اجراء يتم على البيانات الشخصية ويجعل المتعذر الاطلاع عليها أو استعادتها مرة أخرى
10. استخدام البيانات(Data Usage) : يتم تعريف مصطلح استخدام البيانات ضمن سياق حوكمة البيانات بأنه الأسباب الكامنة وراء استغلال البيانات أو المعلومات التي تخص وزارة البيئة والمياه والزراعة. كما يشير المصطلح إلى الأغراض التي قد تُستخدم فيها البيانات من جانب الأفراد. ويجب عدم الخلط بين ذلك وبين استخدام البيانات من جانب عملاء الوزارة بغرض وضع خططهم الخاصة.
11. قنوات الاتصال(Communication Channels) : الوسائل التي يمكن للمرء من خلالها الوصول إلى البيانات أو نقلها أو تبادلها أو مشاركتها داخل الوزارة أو خارجها.
12. البيانات السرية(Confidential Data) : البيانات المتحكم فيها والمحمية وتكون مقتصرة على الاستخدام الداخلي فقط. ويتم تقسيمها إلى بيانات سرية وبيانات سرية للغاية حسب سياسة تصنيف البيانات.
13. مستويات تصنيفات البيانات(Data Classification Level) : التجميع المنطقي للبيانات حسب مستويات الوصول إليها (أنواع البيانات العامة والمقيدة والسرية والسرية للغاية).
14. الراعي الرسمي لحوكمة البيانات: هو وزير وزارة البيئة والمياه والزراعة (أو من يفوض) الذي بدوره يضمن تنفيذ حوكمة البيانات وتفعيلها داخل الوزارة والمراكز التابعة لها. كما أنه يتولى مسؤولية تفعيل اللجنة التوجيهية لحوكمة البيانات ودعمها.
15. مدير ممثل بيانات الأعمال: يتحمل مدير ممثل بيانات الأعمال مسؤولية البيانات الخاصة في قطاعات أو وحدات أعمال محددة (وكالة الزراعة، ووكالة المياه، ووكالة البيئة.)، وحدات وظيفية معينة (مكتب إدارة البيانات، الإدارة العامة للأمن السيبراني، الإدارة العامة لتقنية المعلومات والتحول الرقمي، وما إلى ذلك)، كما يتولى مسؤولية تكليف ممثل بيانات الأعمال الخاص به. كما يتمتع بصلاحية اتخاذ

القرارات المتعلقة ببياناته، متضمنًا ذلك الموافقة على هذه القرارات، وإنفاذها، والالتزام بها بما يقتضي من مصلحة العمل.

16. ممثل بيانات الأعمال: يمثل وحدات الأعمال والوحدات الوظيفية في حوكمة البيانات باعتباره خبيرًا متخصصًا (SME) في العمل ضمن نطاق البيانات الخاص به. كما أنه يضمن فهم السياسات والإجراءات والمعايير والأدوات المتعلقة بحوكمة البيانات واستخدامها في وحدات العمل.
17. مختص بيانات الأعمال: هو عبارة عن خبير متخصص في حوكمة البيانات مهمته ضمان تحديد البيانات المؤسسية واستخدامها في الوزارة على نحوٍ صحيح. كذلك، يتولى تحديد ورصد مدى الامتثال لحوكمة البيانات، والمعايير، والأهداف التي اعتمدتها اللجنة التوجيهية لحوكمة البيانات ولجنة حوكمة البيانات، إضافةً إلى تقديم الدعم لممثلي بيانات الأعمال، وأمناء البيانات، والتنسيق معهم، و إمدادهم بالمعلومات اللازمة.
18. أمين البيانات(Data Custodian) : يتحمّل أمين البيانات المسؤولية عن إدارة العمليات المرتبطة بالبيانات والتنسيق فيما بينها من وجهة نظر النظام. يوجد هذا الدور داخل وحدة التقنية والعمليات، ويجري تنفيذه بالتعاون مع مختص بيانات الأعمال.
19. مستهلك البيانات(Data Consumer) : فرد أو جهة تتلقى مجموعات البيانات وتستخدمها لتنفيذ أنشطة معينة. لا يقوم مستهلكو البيانات بإجراء تغييرات على البيانات في أنظمة المصدر.
20. الامتثال لحوكمة البيانات: عبارة عن لوحة معلومات يُنشئها مسؤول حوكمة البيانات، وتتضمن الجهود المبذولة للامتثال لحوكمة البيانات، وكذلك أيّة استثناءات منحت والأطراف المسؤولة عنها.
21. نطاق البيانات: مجموعة البيانات التي تنتمي إلى غرض محدد من أغراض العمل.
22. خصوصية البيانات(Data Privacy) : هو مفهوم تقييد الوصول غير المصرح به إلى البيانات الخاصة، مثل المعلومات الشخصية، وسجلات العملاء، والبيانات المالية، والمعلومات المتعلقة بالعمل، وغير ذلك.
23. موضوع البيانات: الشخص أو الجهة الذين تشير إليهم البيانات.
24. معلومات التعريف الشخصية (PII): عبارة عن بيانات يمكن استخدامها لتحديد هوية شخص معين أو مكانه. ويجب مراعاة كل خاصية من خصائص البيانات سواء بمفردها أو بالاقتران مع خواص البيانات الأخرى التي يمكن استخدامها لتمييز شخص ما عن شخص آخر، أو استخدامها لإظهار هوية البيانات المجهولة. وتشمل على سبيل المثال الاسم أو رقم التعريف أو بيانات الموقع أو المعرّف عبر الإنترنت أو واحد أو أكثر من العوامل المحددة للعوامل المادية والفسيولوجية، الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية للشخص.
25. معالجة البيانات الشخصية: أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أو يدوية، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكيف

أو التغيير أو الاسترداد أو الاستشارة أو الاستخدام أو الكشف عن طريق النقل أو النشر أو الإتاحة أو المحاذاة أو الدمج أو التقييد أو المحو أو الإتلاف.

26. المتحكّم بالبيانات الشخصية: الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تحدد ، بمفردها أو بالاشتراك مع آخرين ، أغراض ووسائل معالجة البيانات الشخصية ؛ عندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب قوانين المملكة والجهات ذات العلاقة.
27. الاسم المستعار(Pseudonym) : قيمة محسوبة أو مخصصة تحل محل عنصر واحد أو أكثر من عناصر البيانات في سجل صاحب البيانات. ويمثل اسم الشهرة واللقب مصطلحين يشيع استخدامها كاسم مستعار.
28. حجب الهوية(De-identification) : يُقصد بذلك أي عملية تستعمل لإزالة الارتباط القائم بين هوية شخص ما أو جهة معينة، وعناصر البيانات الخاصة بأي منهما. ويمثل إخفاء الهوية واستخدام الأسماء المستعارة نوعين من أنواع حجب الهوية.
29. إعادة تحديد الهوية(Re-identification) : عملية يتم من خلالها تحويل اتجاه البيانات المجهولة أو التي تم حجب هويتها، بحيث يمكن من خلال ذلك تحديد هوية الفرد مرة أخرى.
30. المعرفات الشبيهة: مجموعة من الخصائص التي يمكن أن تعمل القيم المدمجة الخاصة بها بمثابة معرّف لفرد معين.
31. استخدام الأسماء المستعارة(Pseudonymization) : نوع من أنواع إخفاء الهوية عن طريق إزالة الارتباط القائم بين البيانات وصاحب البيانات، وتقديم معرف جديد يُنشئ عملية تعيين متبادلة بين صاحب البيانات والمعرّف الجديد.
32. الاختيار العشوائي(Randomization) : تعمل هذه الآلية على الاحتفاظ بالمعرفات المباشرة (الاسم، ورقم الهاتف)، مع استبدال قيمها لتحل محلها قيم ظاهرية (عشوائية).
33. اخفاء البيانات(Masking) : عملية إزالة أحد المتغيرات أو استبداله، لتحل محله معلومات مستعارة أو مشفَّرة.
34. المعرّفات المباشرة(Direct Identifiers) : عبارة عن البيانات التي تحدد فردًا واحدًا أو صاحب بيانات واحدًا بطريقة مباشرة، دون وجود أي معلومات إضافية، أو عن طريق الربط الشامل للمعلومات الأخرى الموجودة في النطاق العام.
35. المعرفات غير المباشرة(Indirect Identifiers) : تمثل المعرفات غير المباشرة أو الشبيهة البيانات التي لا يمكنها تحديد هوية شخص معين سوى عند استخدامها مع بيانات تحديد الهوية الأخرى غير المباشرة. كذلك، يمكن أن تؤدي المعرّفات غير المباشرة إلى تقليل عدد الأفراد الذين ينتمي إليهم الشخص؛ حيث قد يتم تقليص عددهم إلى فرد واحد في حالة استخدامها معًا.
36. البيانات الخارجية(External Data) : عبارة عن أي بيانات تستخدمها وزارة البيئة والمياه والزراعة أو تحصل عليها من مصادر خارجية لأغراض تتعلق بالعمل. وتشمل الأمثلة عليها البيانات الخاصة بالجهات الشقيقة، وشبكات التواصل الاجتماعي، وبيانات التحقق من العناوين، وبيانات وزارة الداخلية للتحقق من هوية الإقامة، وغير ذلك.

37. البيانات الداخلية(Internal Data) : البيانات التي قد يتم الإفصاح عنها، ورغم أنها ليست محمية على النحو القانوني، إلا أنه لا يجوز إتاحتها للجمهور أو الكشف عنها إلا في ظل ظروف محدودة.
38. البيانات العامة(Public Data) : البيانات المصرح صراحةً أو ضمنًا بتوزيعها على الجمهور دون قيود.
39. البيانات المقيّدة(Restricted Data) : عبارة عن أي معلومات سرية أو شخصية محمية بموجب النظام أو السياسة، وهي تتطلب أعلى مستوى من مستويات التحكم في الوصول والحماية الأمنية، سواء في مرحلة تخزينها أو خلال عملية نقلها.
40. البيانات الحساسة (سرية وسرية للغاية)(Sensitive Data) : عبارة عن معلومات ذات حساسية وسرية عالية. ويجب حماية الوصول إليها؛ حيث قد يؤدي تسريب هذه البيانات إلى رفع دعاوى قضائية، أو قد يكون لذلك تأثير سلبي على العمل، أو الشؤون المالية، أو يؤدي إلى انتهاك خصوصية العملاء.
41. الاسترداد(Recovery) : يُقصد بذلك استرجاع البيانات، والعمليات والأنظمة الخاصة بالعمل لوضعها في حالة تشغيلية ثابتة ومتسقة حسب متطلبات العمل.

1.6. المراجع

- ضوابط ومواصفات مكتب إدارة البيانات الوطنية.
- السياسات الخاصة بحوكمة البيانات الوطنية (سدايا).
- الدليل التنظيمي و النموذج التشغيلي.
- الدليل الإرشادي لتطوير إشعار الخصوصية.
- سياسات الإدارة العامة للأمن السيبراني.
- معيار خصوصية المعلومات الصادر من الأمن السيبراني MWEA-INFOSEC-GOV-STD0010.

2. المبادئ الرئيسية

#	المبدأ	الوصف
1	المسؤولية	أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بالوزارة والمراكز التابعة لها واعتمادها من قبل معالي الوزير (أو من يفوضه)، ونشرها مع جميع الأطراف المعنية بتطبيقها.
2	الشفافية	أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بالوزارة والمراكز التابعة لها يحدد فيه الأغراض التي من أجلها تم معالجة البيانات وذلك بصورة محددة وواضحة وصريحة.
3	الاختيار والموافقة	أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات والحصول على موافقته (الضمنية أو الصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.
4	الحد من جمع البيانات	أن يقتصر جمع البيانات على الحد الأدنى من البيانات الذي يمكّن من تحقيق الأغراض المحددة في إشعار الخصوصية.
5	الحد من استخدام البيانات والاحتفاظ بها والتخلص منها	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 والتشريعات، وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرّح به نظاماً.
6	الوصول إلى البيانات	أن يتم تحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته لمراجعتها، وتحديثها، وتصحيحها.
7	الحد من الإفصاح عن البيانات	أن يتم تقييد الإفصاح عن البيانات للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة.
8	أمن البيانات	أن يتم حماية البيانات من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل، أو الوصول غير المصرّح به - وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
9	جودة البيانات	أن يتم الاحتفاظ بالبيانات بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.
10	المراقبة والامتثال	أن يتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بالوزارة والمراكز التابعة لها، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.
11	تحديد الغرض	يتم جمع البيانات لأغراض محددة وصريحة ومشروعة ولا تتم معالجتها مرة أخرى بطريقة لا تتوافق مع هذه الأغراض وتعتبر المعالجة الإضافية لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية جزء من الأغراض الأولية المسموح بها.
12	الخصوصية في التصميم	الخصوصية في التصميم تضمن أن تعريف وتخطيط جميع الأنظمة الجديدة أو التي تم تغييرها بشكل كبير والتي تجمع البيانات الشخصية أو تعالجها يخضعان إلى الاعتبار الواجب لقضايا الخصوصية، بما في ذلك إكمال حماية البيانات وتقييم الأثر.

3. ضوابط خصوصية البيانات

#	الضوابط	الوصف
1	تقييم الأثر	- النظر في كيفية معالجة البيانات الشخصية ولأي أغراض - تقييم ما إذا كانت المعالجة المقترحة للبيانات الشخصية ضرورية ومتناسبة مع الغرض (الأغراض) - تقييم المخاطر التي يتعرض لها الأفراد في معالجة البيانات الشخصية - ما هي الضوابط اللازمة لمعالجة المخاطر المحددة وإثبات الامتثال للتشريعات
2	نقل البيانات الشخصية	- يجب مراجعة عمليات سرقة البيانات الشخصية بعناية قبل إجراء النقل للتأكد من أنها تقع ضمن منطقة آمنة وتوفر ضمانات كافية بالبيانات الشخصية المطبقة في الدولة المستقبلة وقد يتغير هذا بمرور الوقت. - يجب أن تخضع عمليات نقل البيانات الدولية لاتفاقيات ملزمة قانونًا والتي توفر حقوقًا قابلة للتنفيذ لأصحاب البيانات.
3	مسؤول حماية البيانات	- يجب أن يكون هناك دور محدد لمسؤول حماية البيانات DPO ويجب أن يكون على مستوى مناسب من المعرفة بقوانين حماية البيانات وإدارتها.
4	إشعار تسريب البيانات	- تلتزم الوزارة بأن تكون عادلة ومتناسبة عند النظر في الإجراءات التي يتعين اتخاذها لإبلاغ الأطراف المتضررة بشأن انتهاكات البيانات الشخصية. تماشياً مع اللائحة العامة لحماية البيانات. - عندما يُعرف حدوث انتهاك والذي من المحتمل أن يؤدي إلى خطر على حقوق وحريات الأفراد، سيتم إبلاغ الجهات المسؤولة داخل المملكة في غضون 72 ساعة. - ستتم إدارة عملية إشعار تسريب البيانات وفقًا لإجراءات الاستجابة لحوادث أمن المعلومات الخاصة بالوزارة والتي تحدد العملية الشاملة للتعامل مع حوادث أمن المعلومات.
5	معالجة الامتثال	- يجب أن يكون الأساس القانوني لمعالجة البيانات الشخصية واضح ولا لبس فيه. - يجب أن يتم تعيين مسؤول حماية البيانات بمسؤولية محددة عن حماية البيانات في الوزارة. - جميع الموظفين المشاركين في التعامل مع البيانات الشخصية يجب أن يفهموا مسؤوليات وممارسة حماية البيانات جيدًا. - يجب أن يتم توفير التدريب في مجال حماية البيانات لجميع الموظفين - يتم اتباع القواعد المتعلقة بموافقة أصحاب البيانات - يجب أن يكون هناك طرق متاحة لأصحاب البيانات الذين يرغبون في ممارسة حقوقهم فيما يتعلق بالبيانات الشخصية ويتم التعامل مع هذه الاستفسارات بشكل فعال. - يجب أن تتم عمليات مراجعة دورية للإجراءات الخاصة التي تتعامل مع البيانات الشخصية. - يجب أن يتم اعتماد الخصوصية في التصميم لجميع الأنظمة والعمليات الجديدة أو المتغيرة. - يجب أن يتم تسجيل الوثائق التالية لأنشطة المعالجة: - اسم المنظمة والتفاصيل ذات الصلة. - أغراض معالجة البيانات الشخصية. - فئات الأفراد والبيانات الشخصية التي تمت معالجتها. - فئات متلقي البيانات الشخصية. - الاتفاقيات والآليات الخاصة بنقل البيانات الشخصية إلى دول خارج المملكة بما في ذلك تفاصيل الضوابط المعمول بها. - جداول الاحتفاظ بالبيانات الشخصية. - الضوابط الفنية والتنظيمية ذات الصلة المطبقة

		- يجب أن تتم مراجعة هذه الإجراءات على أساس منتظم كجزء من عملية المراجعة لنظام حماية البيانات.
6	**التزامات الخدمات المقدَّمة**	- يجب أن يُقدَّم للعملاء التسهيلات للوفاء بالالتزامات بموجب القانون في أنشطة مثل الوصول إلى معلومات التعريف الشخصية للأفراد وتعديلها ومحوها. - يجب أن يتم استخدام معلومات تحديد الهوية الشخصية بما يتوافق مع أغراض معالجة البيانات. - يجب أن يتم إبلاغ العميل إذا تم الكشف عن أي من بياناته بموجب القانون، ما لم يكن القيام بذلك محظورًا. - يجب أن يتم تسجيل تفاصيل الإفصاح عن البيانات. - يجب أن يتم إخبار العملاء إذا كان هناك شركاء آخرون لمعالجة معلومات تحديد الهوية الشخصية الخاصة بهم. - يتم إشعار العملاء إن كانت البيانات الشخصية الخاصة بهم عرضة الوصول غير المصرح به.

4. الأدوار والمسؤوليات

دور حوكمة البيانات	المسؤولية
مدير عام مكتب إدارة البيانات	- تسريع القرارات، ومعالجة الخلافات، وتصعيد المشكلات (متى ما أمكن ذلك) لتجنب حالات تعطل العمل. - الإشراف على أعمال حوكمة البيانات كأنشطة معتادة. - مراجعة واعتماد تقرير خرق البيانات وتقديم توصيات.
الإدارة العامة للأمن السيبراني	- للإدارة العامة للأمن السيبراني الدور الهام في هذه السياسة حيث أنها الإدارة القائمة على تتبع كل العمليات التي تتم على البيانات بكافة أنواعها وتصنيفاتها. - تقوم الإدارة العامة للأمن السيبراني بإرسال إشعار حدوث خرق للبيانات الشخصية إلى مسؤول حماية البيانات الشخصية. - تقوم الإدارة العامة للأمن السيبراني بتقييم خرق البيانات وتقديم توصيات إذا كان الخرق يتعلق بأمن المعلومات.
مدير ممثل بيانات الأعمال	- مسؤول البيانات في قطاعات أو وحدات أعمال محددة (وكالة الزراعة، ووكالة المياه، ووكالة البيئة.)، وحدات وظيفية معينة (مكتب إدارة البيانات، الإدارة العامة للأمن السيبراني، الإدارة العامة لتقنية المعلومات والتحول الرقمي، وما إلى ذلك) - يتولى مسؤولية تكليف ممثل بيانات الأعمال الخاص به. كما يتمتع بصلاحية اتخاذ القرارات المتعلقة ببياناته، متضمنًا ذلك الموافقة على هذه القرارات، وإنفاذها، والالتزام بها بما يقتضي مصلحة العمل.
ممثل بيانات الأعمال	- يقوم بتعريف البيانات التي تحتوي على معرفات شخصية. - يقوم بمراجعة طلب صاحب البيانات واعتماده. - تقييم خرق البيانات وتقديم توصيات إذا كان الخرق متعلق بقطاع الأعمال.
الدعم الفني والتقني	- يقوم فريق الدعم الفني والتقني بنقل البيانات الشخصية بحسب الضوابط ذات العلاقة. - ضمان تطبيق التزامات الخدمات المقدمة للحفاظ على خصوصية أصحاب البيانات. - يقوم فريق الدعم الفني والتقني بتطبيق ضوابط حماية البيانات الشخصية بالإضافة إلى تطبيق الضوابط المناسبة لمنع حدوث خروق مستقبلية. - يقوم فريق الدعم الفني والتقني بتقييم خرق البيانات وتقديم توصيات إذا كان الخرق يتعلق بالقطاع الفني.

مختص بيانات الأعمال	- يقوم مختص بيانات الأعمال بتقييم الأثر المترتب على معالجة البيانات الشخصية، بالاستعانة بممثل بيانات الأعمال و وحدة حماية البيانات الشخصية والمستشار القانوني وأمين البيانات. - يقوم مختص بيانات الأعمال بإنشاء خارطة مسار البيانات الشخصية.
وحدة حماية البيانات الشخصية	- تقوم بتطبيق عمليات وسياسات حماية البيانات داخل الوزارة. - معالجة الإجراءات الخاصة بتسريب البيانات. - القيام بالتأكد من الامتثال للسياسات والقوانين الخاصة بحماية البيانات. - تقوم وحدة حماية البيانات الشخصية باستلام وتقييم طلب صاحب البيانات وتنفيذه وإشعار الفرد بتنفيذ الطلب. - تقوم بحفظ طلبات صاحب البيانات في السجلات. - التأكد من مشاركة البيانات الشخصية مع جهات أخرى. - تقوم وحدة حماية البيانات الشخصية بتقييم مخاطر البيانات. - تقوم بتحديد ضوابط حماية البيانات الشخصية و تتأكد من توافقها مع اللائحة العامة لحماية البيانات GDPR. - تقوم بالتأكد من المعلومات والبيانات الشخصية للموردين. - تقوم بتقييم خرق البيانات الشخصية وتحديد الضوابط المناسبة لمنع حدوث خروقات مستقبلية. - إرسال إخطار إلى الأفراد أو الهيئات المشرفة.
الشؤون القانونية	- تتولى الشؤون القانونية مهمة تقييم خرق البيانات وتقديم توصيات إذا كان الخرق يتعلق بالشؤون القانونية.

5. بيان السياسة

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، أرقام الهويات الشخصية، والعناوين، أرقام التواصل، أرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

البيانات الحساسة

كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التى تدل على أن الفرد مجهول الأبوين أو أحدهما.

6. أحكام السياسة

- لا يجوز مشاركة أو معالجة أي معلومات تعريفية وبيانات شخصية تخص العملاء والموظفين وشركاء الأعمال مع أعضاء الوزارة أو أي طرف آخر ما لم يوافق صاحب البيانات على ذلك من خلال التوقيع على نموذج موافقة لهذا الغرض. ويجب أن توضح استمارة الموافقة الغرض من البيانات واستخدامها.
- يحق للفرد/ القطاع تصحيح، إتمام، تحديث أو طلب إتلاف بياناته كما ورد بالتفصيل في (حقوق صاحب البيانات) وذلك من خلال الاتصال بالوزارة، أو استخدام قنوات أخرى للتواصل مع الوزارة في هذا الصدد وعلى الوزارة توفير آلية واضحة تمكنه من ذلك.
- معالجة البيانات الشخصية ومشاركتها إذا طلبت ذلك أحد الجهات يجب توفيرها على النحو المطلوب بعد تصغيرها لمطابقة البيانات المطلوبة فقط ويجوز الإفصاح عن البيانات في الحالات التالية فقط:
-
  - إذا وافق صاحب البيانات الشخصية على الإفصاح وفقاً لما ذكر سابقاً.
  - إذا كانت البيانات الشخصية قد جرى جمعها من مصدر متاح للعموم.
  - إذا كانت الجهة التي تطلب الإفصاح جهة عامة، وذلك لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء ُمتطلبات قضائية وفق الأحكام التي تحددها اللوائح.
  - إذا كان الإفصاح ضروريا لحماية الصحة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم.
  - إذا كان الإفصاح سيقتصر على معالجتها لاحقاً بطريقة لا تؤدي إلى معرفة هوية صاحب البيانات الشخصية أو أي فرد آخر على وجه التحديد.
- يجب أن تكون مشاركة البيانات الشخصية كافية وذات صلة ومحدودة لما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها.
- يجب أن تستند الأذونات الممنوحة لموظفي الوزارة للوصول إلى بيانات الوزارة من خلال أنظمة تكنولوجيا المعلومات إلى واجبات ومسؤوليات الوظيفة لضمان عرض / تحديث / مشاركة بيانات العملاء والمستهلكين فقط إذا كانت هناك حاجة للعمل؛ لحماية خصوصية العملاء والموظفين وشركاء الأعمال.
- يجب أن تحتفظ قطاعات الوزارة والمراكز التابعة لها المختلفة وأنظمة تكنولوجيا المعلومات في الوزارة والمراكز التابعة لها بسجل للأنشطة التشاركية التي تقع تحت مسؤوليتها. يجب أن يحتوي هذا السجل على جميع البيانات التالية:
  - الأسماء
  - أرقام الهواتف والعناوين ومعلومات الاتصال الأخرى
  - الرقم الوطني / رقم الهوية
  - الصور وملفات الوسائط الأخرى

- بصمات الأصابع والصوت
- أي رقم تعريف فريد آخر أو رقم حساب

- يجب على كل موظف بالوزارة والمراكز التابعة لها إخطار مكتب إدارة البيانات فور علمهم بأي خرق للبيانات.
- قد يتم نقل البيانات إلى دولة أخرى أو منظمة دولية إذا سمحت اللوائح السعودية بذلك فقط.
- يجب إجراء تدريب / توعية مناسبة لحماية البيانات لموظفي الوزارة والمراكز التابعة لها من قبل مكتب إدارة البيانات والإدارة العامة لأمن المعلومات.
- يجب معالجة البيانات بطريقة قانونية وعادلة وشفافة.
- يجب أن تكون البيانات دقيقة، ويجب تحديثها عند الضرورة؛ يجب اتخاذ كل خطوة معقولة لضمان أن البيانات غير الدقيقة، مع مراعاة الأغراض التي تتم معالجتها من أجلها، يتم محوها أو تصحيحها دون تأخير.
- معالجة البيانات بطريقة تضمن الأمان المناسب للبيانات، بما في ذلك الحماية ضد المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف أو التلف العرضي، باستخدام التدابير التقنية أو التنظيمية المناسبة.
- على كل الجهات داخل وخارج الوزارة إتلاف البيانات الشخصية فور انتهاء الغرض من جمعها.
- ويجوز لها الاحتفاظ بتلك البيانات بعد انتهاء الغرض من جمعها في الحالات التالية فقط:
  - إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد
  - إذا توافر سبب نظامي يوجب الاحتفاظ بها مدة ُمحددة، وفي هذه الحالة ُيجرى إتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول.
  - إذا كانت البيانات الشخصية متصلة اتّصالا وثيقاً بقضية منظورة أمام جهة قضائية وكان الاحتفاظ بها مطلوباً لهذا الغرض، وفي هذه الحالة ُيجرى إتلافها بعد استكمال الإجراءات القضائية الخاصة بالقضية.

7. العقوبات

- ❖ كل من خالف حكما من أحكام النظام أو اللوائح يعاقب بالإنذار أو بغرامة لا تزيد على خمسة ملايين ريال ويجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة بزيادة الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد.
- ❖ كل من أفصح عن بيانات حساسة أو نشرها مخالفا أحكام النظام، يعاقب بالسجن مدة لا تزيد على سنتين وبغرامة لاتزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية.
- ❖ كل من خالف شروط النقل والإفصاح عن البيانات الشخصية لخارج المملكة يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على مليون ريال، أو بإحدى هاتين العقوبتين.

8. حقوق صاحب البيانات

أولاً: الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته، والغرض من ذلك، وألاَّ تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها والذي من أجله قدّم موافقته الضمنية أو الصريحة.

ثانياً:الحق في الوصول إلى بياناته لدى الوزارة والمراكز التابعة لها، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها بصيغة واضحة.

ثالثاً:يحق لصاحب البيانات طلب تقييد معالجة بياناته الشخصية لحالات خاصة ولفترة زمنية محدودة.

رابعاً:الحق في الرجوع عن موافقته على معالجة بياناته - في أي وقت - مالم يكن هناك أغراض مشروعة تتطلب عكس ذلك.

9. معالجة البيانات الشخصية

هي أي عملية تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية مثل (عمليات التسجيل، الجمع، الفهرسة، ترتيب، التنسيق، التخزين، التعديل، التحديث، الدمج، الاسترجاع، الاستعمال، الإفصاح،النقل، النشر، المشاركة في البيانات أو الربط البيني، الحجب،
المسح، والإتلاف).

9.1. استثناءات في عملية معالجة البيانات الشخصية

- عندما تكون المعالجة مطلوبة لأغراض أمنية أو قضائية.
- عندما تكون المعالجة بمقتضى نظام آخر أو تنفيذاً ا لإتفاق سابق يكون صاحب البيانات الشخصية طرفاً فيه.
- عندما تكون المعالجة لأغراض علمية أو بحثية أو إحصائية وفقا لشروط حددها النظام.
- عندما تحقق المعالجة مصلحة متحققة لصاحب البيانات وكان الاتصال به متعذراً.

9.2. الحالات التي يمكن من خلالها جمع البيانات الشخصية من غيرُ صاحبها مباشرة أو معالجتها لغرض آخر غير الذي جمعت من أجله

- إذا وافق صاحب البيانات الشخصية على ذلك وفقاً لأحكام نظام حماية البيانات الشخصية ولوائحه التنفيذية.
- إذا كانت البيانات الشخصية متاحة للعموم أو جرى جمعها من مصدر متاح للعموم.
- إذا كانت جهة التحكم جهة عامة، وكان جمع البيانات الشخصية من غيرً صاحبها مباشرةً أو معالجتها لغرض آخر غير الذي جمعت من أجله أو مطلوباً لأغراض أمنية أو لتنفيذ نظامٌ آخر أو لاستيفاء متطلبات قضائية.
- إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم.
- إذا كانت البيانات الشخصية لن سجل أو تحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.

10. إنجازات الوزارة تجاه حماية البيانات الشخصية

قامت الوزارة باتخاذ العديد من التدابير والإجراءات الخاصة لحماية البيانات الشخصية وهي:

- إعداد وتطبيق السياسات والإجراءات المتعلقة بحماية البيانات، وسيكون معالي الوزير - أو من يفوضه - مسؤول عن الموافقة عليها واعتمادها.
- إنشاء وحدة لحوكمة البيانات (مرتبطة بمكتب إدارة البيانات والذي تم تأسيسه بموجب الأمر السامي الكريم رقم 59766 وتاريخ 20/11/1439هـ) ويسند لها مسؤولية تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة من الإدارة العليا بالوزارة، على أن تتضمن مهام ومسؤوليات الوحدة وضع المعايير المناسبة لتحديد مستويات حساسية البيانات.
- إعداد وتوثيق الإجراءات اللازمة لإدارة ومعالجة انتهاكات الخصوصية وتحديد المهام والمسؤوليات المتعلقة بفريق العمل المختص، والحالات التي يتم بها إشعار الوزارة ومكتب إدارة البيانات الوطنية حسب التسلسل الإداري - بناءً على قياس شدة الأثر (راجع إدارة عملية خصوصية البيانات).
- إعداد برامج توعوية لتعزيز ثقافة الخصوصية ورفع مستوى الوعي وفقاً لسياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجهة.
- إعداد وتوثيق سياسة وإجراءات الاحتفاظ بالبيانات وفقاً للأغراض المحددة والأنظمة والتشريعات ذات العلاقة.
- إعداد 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 وفقاً لما صدر من الهيئة الوطنية للأمن السيبراني.
- إعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات الشخصية واكتمالها وحداثتها وارتباطها بالغرض الذي جُمعت من أجله.

11. التزامات الوزارة

وللتأكد من استمرارية وجودة مسيرة العمل، تقوم الوزارة ممثلة في مكتب إدارة البيانات بالتعاون مع جميع قطاعات الوزارة والعاملين بها على الالتزام باتباع الآتي:

- تقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات وعرض نتائج التقييم على معالي الوزير - أو من يفوضه - لتحديد مستوى قبول المخاطر وإقرارها.
- مراجعة وتحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية المعتمدة من الإدارة العليا للجهة.
- إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي/الاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة والتشريعات.
- إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
- 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).
- أخذ موافقة صاحب البيانات على معالجة البيانات بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.
- أن يكون الغرض من جمع البيانات متوافقاً مع الأنظمة وذو علاقة مباشرة بنشاط الوزارة والمراكز التابعة لها.
- أن يكون محتوى البيانات مقتصراً على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
- تقييد جمع البيانات على المحتوى المعد سلفاً ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
- أن يقتصر استخدام البيانات على الغرض الذي جُمعت من أجله.
- تخزين البيانات ومعالجتها داخل الحدود الجغرافية للمملكة لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات، ولا يجوز معالجتها خارج المملكة إلا بعد حصول الجهة المستفيدة على موافقة كتابية من الوزارة، بعد التنسيق مع مكتب إدارة البيانات الوطنية.
- تضمين أحكام سياستي الاحتفاظ والتخلص من البيانات في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.
- تحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته وذلك لمراجعتها وتحديثها.
- التحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقاً للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
- حظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقاً للأغراض المحددة بعد موافقة صاحب البيانات ووفقاً للأنظمة والتشريعات على أن يتم تزويد الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة وتضمينها في العقود والاتفاقيات.

- إشعار أصحاب البيانات وأخذ الموافقة منهم في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.
- يقوم مكتب إدارة البيانات - بعد التنسيق مع معالي الوزير - بأخذ موافقة مكتب إدارة البيانات الوطنية قبل مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة.
- استخدام الضوابط الإدارية والتدابير التقنية المعتمدة في سياسات الوزارة لأمن المعلومات لضمان حماية البيانات الشخصية ومنها على سبيل المثال لا الحصر:
  - منح صلاحيات الوصول إلى البيانات وفقاً 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 وفقاً للسياسات والإجراءات والأنظمة والتشريعات.
  - اختيار العاملين الذين يباشرون عمليات معالجة البيانات ممن يتصفون بالأمانة والمسؤولية ووفقاً لطبيعة وحساسية البيانات وسياسة الوصول المعتمدة من قبل الوزارة.
  - استخدام التدابير الأمنية المناسبة - كالتشفير، وعزل بيئة التطوير والاختبار عن بيئة التشغيل - لأمن البيانات وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
- مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على معالي الوزير - أو من يفوضه - كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال و رفعها لمعالي الوزير ومكتب إدارة البيانات الوطنية حسب التسلسل التنظيمي.

12. أحكام عامة

أولاً: تتولى الوزارة والمراكز التابعة لها مواءمة أحكام هذه السياسة مع وثائقها التنظيمية وتعميمها على جميع الجهات التابعة لها أو المرتبطة بها بما يحقق التكامل ويضمن تحقيق الهدف المنشود من إعداد هذه السياسة.

ثانياً: تقوم الوزارة والمراكز التابعة لها بمراقبة الامتثال لهذه السياسة بشكل دوري.

ثالثاً: يجب على جميع الجهات التابعة للوزارة الامتثال لهذه السياسة وتوثيق الامتثال وفقاً للآليات والإجراءات التي تحددها الوزارة.

رابعاً: يجب على جميع الجهات التابعة للوزارة إبلاغ الوزارة فوراً ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقاً للآليات والإجراءات التي تحددها الوزارة.

خامساً: يجب على جميع الجهات التابعة للوزارة عند تعاقدها مع جهات خارجية أن تتحقق بشكل دوري من امتثال هذه الجهات لكل السياسات المذكورة بهذة الوثيقة وفقاً للآليات والإجراءات التي تحددها الوزارة، على أن يشمل ذلك أي تعاقدات لاحقة تقوم بها تلك الجهات خارجية.

سادساً: يحق للوزارة وضع قواعد إضافية لمعالجة أنواع محددة من البيانات وفقاً لطبيعة وحساسية هذه البيانات بعد التنسيق مع مكتب إدارة البيانات الوطنية.

سابعاً: تقوم الوزارة - بعد التنسيق مع مكتب إدارة البيانات الوطنية - بإعداد الآليات والإجراءات التي تنظم عملية معالجة الشكاوى وفقاً لإطار زمني محدد وحسب التسلسل التنظيمي لها.

ثامناً: يقوم مكتب إدارة البيانات الوطنية بوضع المعايير اللازمة التي تساعد جميع الجهات التابعة للوزارة على معرفة ما إذا كان تعيين مسؤول حماية بيانات يعتبر متطلب أساسي أو اختياري.

13. الإرشادات

وللتأكد من استمرارية وجودة مسيرة العمل، تقوم الوزارة ممثلة في مكتب إدارة البيانات بالتعاون مع جميع قطاعات الوزارة والعاملين بها على الالتزام باتباع الآتي:

- تضمن حماية البيانات أن البيانات الحساسة وفقًا لسياسات مكتب إدارة البيانات الوطنية وسياسات الأمن السيبراني ومعايير تصنيف المعلومات والتعامل معها التابعة للوزارة تخضع لمستوى مناسب من الحماية.
- تعتبر نطاقات البيانات التالية ذات أهمية كبيرة، ويجب أن تخضع لمستوى مناسب من مستويات حماية البيانات:
  - معلومات التعريف الشخصية (PII)
  - بيانات كبار الشخصيات
  - بيانات الجهات الحكومية
  - البيانات المؤسسية الحساسة لوزارة البيئة والمياه والزراعة
- يتحمل مدير ممثل بيانات الأعمال وممثل بيانات الأعمال المسؤولية عن الامتثال لسياسة الأمن السيبراني، وسياسة خصوصية بيانات الموظفين، وسياسة خصوصية بيانات العملاء التابعة للوزارة، واعتماد معيار تصنيف المعلومات والتعامل معها.
- يتحمل مدير ممثل بيانات الأعمال المسؤولية عن التأكد من توافق جميع معلومات التعريف الشخصية، وبيانات كبار الشخصيات، وبيانات الجهات الحكومية، والبيانات المؤسسية الحساسة لوزارة البيئة والمياه والزراعة، مع السياسات والمعايير والإرشادات الصادرة عن جميع الهيئات التنظيمية.

13.1. مصفوفة تصنيف البيانات الشخصية

النطاق	التصنيف			
	معلومات سري للغاية	معلومات سرية	معلومات مقيد	معلومات عامة
معلومات التعريف الشخصية (الحساسة)		✔		
بيانات الشخصية غير الحساسة			✔	
بيانات كبار الشخصيات		✔		
بيانات كبار الشخصيات			✔	
البيانات المؤسسية الحساسة للوزارة		✔		

13.2. معلومات التعريف الشخصية (PII)

- يتحمل مدير ممثل بيانات الأعمال المسؤولية عن تحديد البيانات التي تنتمي إلى نطاق البيانات الخاص به وحمايتها خلال مراحل دورة حياتها.
- يتحمل مدير ممثل بيانات الأعمال وممثل بيانات الأعمال المسؤولية عن تصنيف البيانات وفقًا لسياسة تصنيف البيانات.

13.3. بيانات كبار الشخصيات

- يتحمل مدير ممثل بيانات الأعمال المسؤولية عن تحديد بيانات كبار الشخصيات التي تنتمي إلى نطاق البيانات الخاص به وحمايتها.
- يتحمل مدير ممثل بيانات الأعمال وممثل بيانات الأعمال المسؤولية عن التأكد من تصنيف بيانات كبار الشخصيات في فئتها المناسبة وفقًا لسياسة تصنيف البيانات.

13.4. بيانات الجهات الحكومية

- يتحمل مدير ممثل بيانات الأعمال المسؤولية عن تحديد بيانات الجهات الحكومية التي تنتمي إلى نطاق البيانات الخاص به وحمايتها.
- يحرص مدير ممثل بيانات الأعمال وممثل بيانات الأعمال على تصنيف بيانات الجهات الحكومية ضمن فئة البيانات المقيدة وفقًا لسياسة تصنيف البيانات.

13.5. البيانات المؤسسية الحساسة

- يتحمل مدير ممثل بيانات الأعمال المسؤولية عن تحديد البيانات المؤسسية الحساسة الخاصة بألوزارة والتي تنتمي إلى نطاق البيانات الخاص به وحمايتها.
- يتحمل مدير ممثل بيانات الأعمال وممثل بيانات الأعمال المسؤولية عن التأكد من تصنيف البيانات المؤسسية الحساسة في فئتها المناسبة وفقًا لسياسة تصنيف البيانات.

وزارة البيئة والمياه والزراعة
Ministry of Environment Water & Agriculture

نسعد باستقبال استفساراتكم واقتراحاتكم عبر إيميل

مكتب إدارة البيانات:

dmo@mewa.gov.sa