A

联合国粮食及农业组织 | Food and Agriculture Organization of the United Nations | Organisation des Nations Unies pour l'alimentation et l'agriculture | Продовольственная и сельскохозяйственная организация Объединенных Наций | Organización de las Naciones Unidas para la Alimentación y la Agricultura | منظمة الأغذية والزراعة للأمم المتحدة

لجنة الشؤون الدستورية والقانونية

الدورة الخامسة عشرة بعد المائة

روما، 21–23 مارس/آذار 2022

معلومات محدثة عن سياسات منظمة الأغذية والزراعة بشأن حماية البيانات وحقوق الملكية الفكرية

أولًا– معلومات أساسية

1- دعا المجلس، في دورته الخامسة والستين بعد المائة، إلى تعزيز أطر منظمة الأغذية والزراعة (المنظمة) المتعلّقة بحماية البيانات وحقوق الملكية الفكرية، لا سيما في سياق مبادرة العمل يدًا بيد،[1] والاستراتيجية الجديدة لإشراك القطاع الخاص،[2] والإطار الاستراتيجي الجديد، واستجابة المنظمة لجائحة كوفيد-19.[3] وذكّر المجلس، في دورته السادسة والستين بعد المائة، بالحاجة إلى "*وضع سياسة شاملة للبيانات بما يضمن حوكمة البيانات، وتكامل البيانات وخصوصيتها إضافةً إلى حقوق الملكية الفكرية، والامتثال للمعايير والبروتوكولات المتفق عليها دوليًا*".[4]

2- وفي ما بعد، أيّد المجلس في دورته الثامنة والستين بعد المائة، "*نتائج اللجنة واستنتاجاتها في ما يتعلّق بالمبادئ التوجيهية بشأن حماية البيانات والملكية الفكرية التي من شأنها أن تشكّل معالم عملية وضع إطار عمل المنظمة حول حماية البيانات وحقوق الملكية الفكرية، وإذ لاحظ اهتمام أعضاء المنظمة والتزامهم بهذه المسألة*"،[5] سلّط الضوء على "*مدى أهمية وضع السياسات بالتشاور مع الأعضاء، وأوصى إدارة المنظمة باتخاذ الترتيبات اللازمة لإجراء المزيد من المشاورات الشاملة مع الأعضاء بغية توضيح وثيقة إطار العمل ووضعها في صيغتها النهائية، بما في ذلك من خلال الأجهزة الرئاسية للمنظمة، حسب الاقتضاء*".[6]

[1] الفقرة 14(ط) من الوثيقة CL 165/REP

[2] الفقرة 11(ي) من الوثيقة CL 165/REP

[3] الفقرة 13(ج) من الوثيقة CL 165/REP

[4] الفقرة 24(ك) من الوثيقة CL 166/REP

[5] الفقرة 30(د) من الوثيقة CL 168/REP

[6] المرجع نفسه.

3- وفي يوليو/تموز 2021، أصدرت الإدارة طلبًا عبر بوابة الأعضاء لالتماس الآراء بشأن المسائل التي اعتبر الأعضاء أنه يجب معالجتها في إطار العمل حول حماية البيانات. وبعد تلقي مساهمات قيّمة، ولدى النظر في بعض الملاحظات والتساؤلات المقدمة، تم عقد جلسة إحاطة غير رسمية عن حماية البيانات والملكية الفكرية في أكتوبر/تشرين الأول 2021 شارك فيها جميع الأعضاء. وفي نوفمبر/تشرين الثاني 2021، أعادت الإدارة توجيه دعوة إلى الأعضاء لتقديم المزيد من الإسهامات الخطية.

4- وفي ضوء التوصيات التي قدمتها الأجهزة الرئاسية، عقدت الإدارة جلسة إحاطة غير رسمية أخرى في 7 مارس/آذار 2022 لإطلاع الأعضاء على التقدم المحرز والتماس تعليقاتهم. وسوف يعقد اجتماع غير رسمي مشترك بين لجنة الشؤون الدستورية والقانونية ولجنة البرنامج في 18 مارس/ آذار 2022 لمناقشة بصفة خاصة البند المتعلق بحوكمة الأنشطة الإحصائية ومواءمة السياسات بشأن حماية البيانات والملكية الفكرية.

ثانيًا– سياسة حماية البيانات

5- تشتمل مسودة السياسة الداخلية بشأن حماية البيانات (السياسة) المرفقة بهذه الوثيقة على المبادئ التوجيهية بشأن حماية البيانات (مبادئ حماية البيانات)، وتتناول تصنيف البيانات إضافة إلى المسؤوليات وآلية الرقابة القائمة داخل المنظمة. وستطبق هذه السياسة على جميع أنشطة المنظمة وعملياتها التي تنطوي على معالجة البيانات الشخصية وغير الشخصية من جانب المنظمة. ولقد تم وضع المسودة مع مراعاة التوجيهات الصادرة عن لجنة الشؤون الدستورية والقانونية في دورتها الثالثة عشرة بعد المائة، والمعلومات والآراء الواردة من الأعضاء عبر العمليات التشاورية الوارد ذكرها أعلاه. ولقد تم أيضًا أخذ المعايير الدولية وما يعادلها من صكوك وضعتها وكالات فردية تابعة لمنظومة الأمم المتحدة، والصكوك التي تم وضعها عن طريق تنسيق منظومة الأمم المتحدة، في الاعتبار.

6- وفي حين أن السياسة تهدف إلى تقديم القدر الكافي من التوجيهات لتمكين الموظفين من تطبيق المبادئ بشكل مباشر على أنشطتهم الرسمية، إلا أنها ستُستكمل بخطوط توجيهية تشغيلية وإجراءات مفصلة تتناول أنواعًا محددة من الأنشطة أو البيانات. ويجري حاليًا استعراض الإجراءات المفصلة القائمة، وسيستمر استعراضها، لضمان اتساقها مع السياسة.[7]

ثالثًا– سياسة الملكية الفكرية

7- بالرغم من أن مسودة سياسة حماية البيانات تتناول البيانات الشخصية وغير الشخصية وتغطي بالتالي بعض جوانب حقوق الملكية الفكرية، فإنه يجري إعداد صك منفصل يتناول إدارة حقوق الملكية الفكرية من جانب المنظمة. وسيتضمن هذا الصك المبادئ التوجيهية المتعلّقة بحقوق الملكية الفكرية التي استعرضتها لجنة الشؤون الدستورية والقانونية، والمعلومات والآراء الواردة من الأعضاء، بالإضافة إلى الممارسات والمعايير الدولية وتلك المعتمدة في منظومة الأمم المتحدة.

[7] على سبيل المثال الأقسام 702 (التحويلات النقدية) و340 (ملفات الموظفين السرية) و502 (توريد السلع والأشغال والخدمات) و505 (تكنولوجيا المعلومات) و601 (إدارة الأرشيف والسجلات) من دليل التعليمات الإدارية.

رابعًا– الإجراء المقترح اتخاذه من جانب اللجنة

8- إن اللجنة مدعوة إلى الإحاطة علمًا بالتقدم المحرز في وضع إطار عمل المنظمة حول حماية البيانات وحقوق الملكية الفكرية. وقد ترغب اللجنة، على وجه الخصوص، في الإحاطة علمًا بمسودة سياسة حماية البيانات وتقديم التعليقات عليها.

الملحق الأول

مسودة سياسة حماية البيانات

تعميم إداري

رقم XX/2022

التاريخ: XX مارس/آذار 2022

سياسة حماية البيانات

أولًا– مقدمة

1- وفقًا للمادة 1 من الدستور، تتمثل إحدى وظائف منظمة الأغذية والزراعة في "*جمع المعلومات المتعلّقة بالتغذية والأغذية والزراعة وتحليلها وتفسيرها ونشرها*".[8] ويشير الإطار الاستراتيجي للفترة 2022–2031 أيضًا إلى أن إحدى الوظائف الأساسية للمنظمة تتمثل في "*تجميع وتحليل ورصد وتحسين الوصول إلى البيانات والمعلومات في المجالات المتعلّقة بولاية المنظمة*" وفي "*الدعوة والاتصال على المستويات الوطنية والإقليمية والعالمية، بما في ذلك بالمستهلكين، مع الاستفادة من معارف المنظمة وبياناتها وموقعها كوكالة متخصصة تابعة للأمم المتحدة ودورها الموثوق كوسيط محايد*".[9]

2- وتُعدّ البيانات أصولًا استراتيجية لتنفيذ ولاية المنظمة. ويجب أن تكون هذه الأخيرة قادرة على استخدام هذه الأصول من دون تقويضها أو تعريضها للخطر. ومن الأهمية بمكان أن يكون هناك سياسة خاصة بحماية البيانات لكفالة حماية البيانات التي تعالجها المنظمة وضمان قيمتها واستخدامها وسلامتها.

3- وينبغي لأي بيانات[10] تستخدمها المنظمة أو تعالجها أو تنقلها إلى طرف ثالث، أن تعالج بشكل صحيح ومتسق طيلة دورة حياتها، أي من لحظة جمعها الأولي وتخزينها إلى حين حذفها.

---

[8] المادة 1(1) من الدستور.

[9] الفقرة 43 من الإطار الاستراتيجي لمنظمة الأغذية والزراعة للفترة 2022-2031.

[10] انظر الفقرة 9 أدناه والملحق الأول بعنوان "التعاريف".

4- ويعرّض الإفصاح غير المصرّح له عن البيانات وسوء استخدامها ومعالجتها بطريقة غير ملائمة، ومعالجة البيانات ذات النوعية الرديئة، المنظمة لمخاطر قانونية ومالية وتشغيلية ومتعلّقة بالسمعة. وتساهم سياسة حماية البيانات التي يتم تنفيذها بشكل صحيح في تعزيز الثقة بالمنظمة وبعملها. ومن الضروري أن تحظى أي بيانات في حوزة المنظمة أو تعهد بها هذه الأخيرة إلى طرف ثالث، بحماية ملائمة.

5- وللتخفيف من المخاطر وتعزيز الحماية، تحدد هذه السياسة مبادئ المنظمة المتعلّقة بحماية البيانات والتي ترد بالتفصيل في القسم الثالث أدناه. وتتواءم هذه المبادئ الشاملة مع المبادئ والضوابط الدولية المتعلّقة بحماية البيانات، بما في ذلك مبادئ منظومة الأمم المتحدة[11] وضوابطها، وتنطبق على كامل دورة حياة معالجة البيانات أي: كيف يتم جمع البيانات، وكيف يجب حفظها ومعالجتها، وكيف ومتى يجب حذفها.

6- وكما هو مفصّل في القسم الثالث، فإن مبادئ حماية البيانات هي:

- ✓ النزاهة
- ✓ السلامة
- ✓ المسؤولية
- ✓ الأمن
- ✓ الشفافية

7- وتعتبر مبادئ حماية البيانات وما ينشأ عنها من التزامات، رفيعة المستوى وحيادية في ما يتعلّق بالتكنولوجيا. ولذلك، فإنها تتيح المرونة اللازمة في تطبيقها اليومي. وينبغي للموظفين أن يترجموا هذه المبادئ إلى تدابير وأدوات تلبّي احتياجاتهم المحددة للعمل وتؤمن في الوقت نفسه مستوى متناسبًا من الحماية للبيانات التي يعالجونها. وسيتم إصدار توجيهات تشغيلية إضافية في إطار هذه السياسة يكون من شأنها معالجة أنواع محددة من الأنشطة التي تتطلب معالجة البيانات.

ثانيًا– النطاق والتطبيق

8- نظرًا إلى الوضع القانوني للمنظمة، بصفتها وكالة متخصصة تابعة للأمم المتحدة، وامتيازاتها وحصاناتها وإلى عدم انطباق القوانين الوطنية أو الإقليمية على أنشطتها، تحدد هذه السياسة المبادئ والقواعد الشاملة التي تنظم معالجة البيانات وحمايتها من جانب المنظمة.[12]

---

[11] انظر مثلًا *"استراتيجية بيانات الأمين العام للأمم المتحدة من أجل العمل من قبل الجميع، في كل مكان بتبصّر وتأثير ونزاهة"* و*"مبادئ الأمم المتحدة بشأن حماية البيانات الشخصية وخصوصيتها"*.

[12] تطبق هذه السياسة مع إيلاء العناية الواجبة للخصائص الرئيسية للمنظمة، بما في ذلك وضعها الحكومي الدولي، وحيادها، وما لديها من سلطة لتوفير منتدى محايد يمكن فيه للدول أن تدعو كل منها الأخرى للحوار ولتبادل المعرفة وسلطة للطلب من أي من الأعضاء تقديم معلومات متصلة بغرض المنظمة. انظر النصوص الأساسية للمنظمة، بما في ذلك المادتين 1 و6 من الدستور من جملة مواد أخرى، والإطار الاستراتيجي للمنظمة للفترة 2022-2031.

9- ولا تنطبق هذه السياسة على البيانات العامة، كما هو مبيّن في الفقرة 14، ولا على البيانات المجهولة المصدر، كما يجري تعريفها في الملحق الأول. وتنطبق هذه السياسة على جميع البيانات الأخرى بشتى أشكالها[13]، بما في ذلك البيانات الشخصية وغير الشخصية التي يفصح عنها شخص اعتباري أو طبيعي للمنظمة أو التي تصدر عن المنظمة.[14]

10- وتنطبق هذه السياسة على جميع الأنشطة والعمليات التي تنطوي على معالجة البيانات من جانب المنظمة أو من جانب أطراف ثالثة في نطاق تعاملها مع المنظمة. ويتعيّن على جميع الموظفين معالجة البيانات بما يتفق مع هذه السياسة. ويجب تنفيذ جميع القواعد والسياسات الداخلية الأخرى التي تتناول جوانب محددة من حماية البيانات، وتفسيرها وفقًا لهذه السياسة. وفي حال وجود أي تعارض، تكون الغلبة لهذه السياسة.

11- وتحدد هذه السياسة المعايير الدنيا لحماية البيانات التي تولّدها المنظمة أو التي يُعهد بها إليها من جانب شخص اعتباري أو فرد (أي مزود للبيانات). كما أنها تنشئ الآليات المؤسسية الداخلية للإشراف على تطبيق مبادئ حماية البيانات ولرصد هذه السياسة حتى تبقى ملائمة للغرض منها. ويرد تعريف المصطلحات المستخدمة في هذه السياسة في **الملحق الأول**، فيما ترد في **الملحق الثاني** الأمثلة على كيفية تطبيق مبادئ حماية البيانات.

[13] بالشكل المطبوع أو الرقمي

[14] تطبق هذه السياسة بغض النظر عما إذا كانت البيانات مقدمة من الفرد الذي تتم معالجة بياناته أو من كيان مختلف (مثلًا عندما يقوم عضو بتقديم معلومات عن الأفراد الخاضعين لولايته القانونية).

ثالثًا– المبادئ الخمسة لحماية البيانات

1– النزاهة

"نعالج البيانات بالاستناد إلى أساس شرعي ولغرض محدد فقط. ولا نجمع ونحتفظ سوى بالقدر الأدنى من البيانات التي نحن بحاجة إليها"

1–1 النقاط الرئيسية

النزاهة تعني أن المنظمة تعالج البيانات بطرق يمكن أن يتوقعها مزود البيانات بصورة معقولة. ويتطلب ذلك تحديد أساس شرعي لعملية المعالجة وتوضيح الغرض التجاري بشكل جيد. ولا يجب أن تجمع المنظمة سوى القدر الأدنى من عناصر البيانات اللازمة لمثل هذا الغرض. ولا يجوز الاحتفاظ بالبيانات بعدما يتم تحقيق هذا الغرض.

2–1 المسؤوليات

1–2–1 الأساس الشرعي

لا يجوز للموظفين معالجة البيانات إلا في إطار الأنشطة المضطلع بها في سياق ولاية المنظمة وبما يتماشى مع إطارها القانوني. وبالإضافة إلى التأكد مما ذكر أعلاه، يجب أن يهيّئ الموظفون أحد الأسس الشرعية التالية لمعالجة البيانات: (1) موافقة مزود البيانات المسبقة عن علم؛[15] (2) أو المصالح الحيوية للفرد في حال تعذّر الحصول على موافقة مسبقة عن علم؛[16] (3) أو الحاجة إلى تطبيق اتفاق قانوني أبرم قبل معالجة البيانات (مثلًا لتنفيذ شروط عقد العمل المبرم).

1–2–2 تحديد الغرض

يجب تحديد الغرض المعيّن من معالجة البيانات قبل جمعها.

1–2–3 المعالجة الإضافية

لا تجوز معالجة البيانات لغرض جديد إلا إذا استوفت هذه العملية شرطًا واحدًا أو أكثر من الشروط التالية: (1) تتفق مع الغرض الأساسي؛ (2) لديها أساسها الشرعي الخاص؛ (3) تستند إلى تعبير جديد عن الموافقة في حال شكّلت الموافقة الأساس الشرعي الأولي؛ (4) ترتبط بالأنشطة الإحصائية أو البحثية المضطلع بها لتحقيق الولاية الفنية للمنظمة؛ (5) تجرى لأغراض الحفظ بموجب القسم 601 من دليل التعليمات الإدارية بشأن إدارة الأرشيف والسجلات.

1–2–4 الضرورة

يجب، بالقدر الممكن عمليًا، جمع ومعالجة الكم الأدنى فقط من البيانات اللازمة لتحقيق الغرض المحدد. ولا يجوز جمع أو معالجة البيانات غير الضرورية أو الزائدة أو التي لا صلة لها بالغرض.

---

[15] يجوز لمزود البيانات أن يسحب موافقته. ويمكن الاطلاع على التوجيهات المتعلّقة بمعالجة سحب الموافقة في الفقرة 33–ج. انظر أيضًا معالجة البيانات الحساسة في الفقرة 24 أدناه.

[16] في الحالات الاستثنائية التي لا يكون فيها الحصول على موافقة عن علم ممكنًا – مثلًا عندما تكون معالجة البيانات ضرورية لحماية حياة الأفراد أو سلامتهم أو صحتهم أو أمنهم، أو حياة أشخاص آخرين أو سلامتهم أو صحتهم أو أمنهم – تجوز معالجة البيانات على أساس المصلحة الحيوية. ويجب تسجيل أسباب عدم الحصول على الموافقة عن علم بالكامل واستعراضها بصورة منتظمة للتأكد من أن الظروف التي حالت دون الحصول على هذه الموافقة لم تتغيّر. وعلى سبيل المثال، لا تعفي الظروف الاستثنائية كتلك الموظفين من الامتثال لجميع العناصر الأخرى الواردة في هذه السياسة.

1-2-5 الاحتفاظ بالبيانات

لا يجوز الاحتفاظ بالبيانات إلا للمدة اللازمة لتحقيق الغرض الذي جمُعت من أجله. وعندما يتم تحقيق هذا الغرض، وما لم تكن البيانات تعالج لأغراض إحصائية أو بحثية أو لأغراض الحفظ، فإنه يجب حذفها أو جعل مصدرها مجهولًا، حسب الاقتضاء، في مهلة معقولة بعد تحقيق الغرض. ويجوز تخزين البيانات لفترة أطول من الفترة اللازمة لتحقيق الغرض الذي جمُعت من أجله بقدر ما يكون هناك غرض مشروع من الاحتفاظ بها (مثل التقيّد بفترات الاحتفاظ التي تفرضها قواعد المنظمة أو الاتفاقات التي تبرمها هذه الأخيرة مع البلدان المستفيدة والشركاء في الموارد).

1-2-6 عمليتا الاحتفاظ بالبيانات وحذفها

يجب أن يطبّق الموظفون المعايير والعمليات والأدوات المناسبة لضمان الاحتفاظ بالبيانات لفترة محدودة وحذفها في ما بعد.

1-2-7 احتفاظ طرف ثالث بالبيانات

عندما يتم نقل البيانات إلى طرف ثالث، يجب أن يكفل الموظفون أن يكون هذا الطرف ملزمًا بموجب العقد بإتلاف جميع البيانات المنقولة إليه أو إعادتها إلى المنظمة ما أن يتحقق الغرض من نقلها أو عند إنهاء الاتفاق الذي نُقلت بموجبه أو انقضاء مدته، إلا إذا كان الطرف الثالث حاصل على موافقة مزود البيانات الصريحة على مواصلة عملية المعالجة.

2- السلامة

"نتحقق من أن البيانات دقيقة. ونحذف أو نصحح أي بيانات غير دقيقة أو غير موثوق بها"

2-1 النقاط الرئيسية

السلامة تعني تطبيق العمليات والضوابط الهادفة إلى كفالة دقة البيانات بشكل عام. وهذا أمر مطلوب لضمان استخدام البيانات وتفسيرها بشكل فعال. ويجب أن يتّخذ الموظفون، قبل جمع البيانات وطيلة دورة حياتها، تدابير معقولة لكفالة دقة البيانات التي يعالجونها وموثوقيتها. وإذا ثبت، لأي سبب كان وفي أي وقت كان، أن البيانات غير دقيقة أو مضللة، فإنه يجب اتخاذ تدابير فورية لضمان تصحيحها أو حذفها.

2-2 المسؤوليات

2-2-1 الموجبات العامة

الموظفون مسؤولون بصفة فردية عن دقة البيانات التي يعالجونها. ولذلك، يجب أن يتخذوا جميع التدابير المعقولة لكفالة دقة البيانات.

2-2-2 تسجيل البيانات وحذفها

يجب اتخاذ جميع التدابير المعقولة من أجل: (1) تسجيل ومعالجة البيانات الدقيقة فقط، (2) وضمان حذف أي بيانات غير دقيقة أو تصحيحها من دون إبطاء.

2-2-3 الاستعراض

يجب تهيئة عمليات لاستعراض دقة البيانات بصورة منتظمة بهدف تجنّب الأخطاء أو التناقضات والتقليل منها.

3– المسؤولية

"نمتثل بشكل استباقي للمبادئ الخمسة لحماية البيانات ويمكننا أن نثبت امتثالنا لها"

3–1 النقاط الرئيسية يجب على جميع الموظفين الامتثال لمبادئ حماية البيانات والتمكن من إثبات أنهم اتخذوا تدابير معقولة لضمان الامتثال لهذه السياسة وللخطوط التوجيهية والإجراءات ذات الصلة التي حددتها المنظمة.

3–2 المسؤوليات

3–2–1 الموجبات العامة يجب اتخاذ تدابير مناسبة ومتكافئة لضمان وإثبات أن البيانات تعالج وفقًا لهذه السياسة. وقبل معالجة البيانات، يجب اتخاذ التدابير لتصميم عملية المعالجة بطريقة تسمح بالحؤول دون تعرّض مزود البيانات والمنظمة للمخاطر أو بالتقليل منها. ويجب أن تكفل هذه التدابير أيضًا عدم جمع بيانات غير تلك اللازمة لتحقيق الغرض المحدد. ويجب أن تُستعرض هذه التدابير بشكل منتظم وأن يتم تحديثها حسب الاقتضاء.

3–2–2 الأدلة على الامتثال يجوز استخدام الإجراءات التالية لإثبات الامتثال لهذه السياسة:

- حفظ سجلات محدّثة لأنشطة المعالجة تشمل على الأقل معلومات عن الغرض من المعالجة، والبيانات التي تتم معالجتها، ومستوى سرّيتها، وحسب الاقتضاء، المستفيدين من البيانات (الداخليين والخارجيين على السواء)، والفترات المتوقعة للاحتفاظ بالبيانات، والتدابير الأمنية المتخذة.
- إجراء تقييم ("تقييم تأثير حماية البيانات")، قبل معالجة البيانات، لتحديد المخاطر ومعالجتها والتخفيف منها في حال كان من المرجح أن تعرّض عملية المعالجة مزود البيانات أو المنظمة لمخاطرة عالية. ولتقييم ما إذا كانت عملية المعالجة تنطوي على مخاطرة عالية، يحدد الموظفون مدى إمكانية تعرّض مزود البيانات أو المنظمة لأي ضرر محتمل ومدى فداحة هذا الضرر. وعندما يتقرر أنه من المحتمل أن تعرّض عملية المعالجة مزود البيانات أو المنظمة لخطر عال، يجب استشارة وحدة حماية البيانات[17] لالتماس مشورتها وتوجيهاتها في ما يتعلّق بتدابير التخفيف المحتملة وتنفيذها.
- تصميم عملية المعالجة بطريقة تسمح بالحؤول دون التعرّض للمخاطر التي تم تحديدها، أو بتجنّبها أو التقليل منها.
- تنفيذ العمليات والإجراءات لمعالجة طلبات مزودي البيانات والاستجابة لها.

[17] انظر الفقرة 44 أدناه.

- تطبيق عمليات وأساليب وتقنيات تكفل مستوى من الأمن يتناسب مع مستوى السرّية المصنّف وفقًا للقسم الرابع أدناه. ويمكن أن تشمل هذه الخطوات حجب الهوية، أو استخدام الأسماء المستعارة، أو التشفير (أنظر **الملحق الأول**).

4– الأمن

"نحمي البيانات باتخاذ إجراءات معقولة ضد التهديدات الخارجية والداخلية"

4–1 النقاط الرئيسية تعتبر المنظمة مسؤولة عن البيانات التي تعالجها ويجب على الموظفين فيها أن يتخذوا تدابير أمنية معقولة لحمايتها. ويجب أن تحافظ هذه التدابير على سرّية البيانات بمنع الإفصاح عنها أو استخدامها بطريقة غير مصرّح لها، وأن تحفظ سلامة البيانات من خلال منع تعديلها غير المصرّح له وإتاحة الوصول المصرّح له فقط. ويكون جميع الموظفين مسؤولين بصفة فردية عن تقييم المخاطر الناشئة عن أي عملية محددة لمعالجة البيانات وعن ضمان اتخاذ التدابير الأمنية المعقولة.

4–2 المسؤوليات

4–2–1 الموجبات العامة يجب على الموظفين حماية البيانات التي يعالجونها وفقًا لأقسام دليل التعليمات الإدارية المعنية والمنشورات الإدارية ذات الصلة.

4–2–2 التدابير الأمنية المناسبة يجب اعتماد التدابير والإجراءات والضوابط الأمنية التنظيمية والمادية والفنية المناسبة لحماية البيانات، تبعًا لمستوى سرّية هذه الأخيرة. ويجب أن تكون هذه التدابير والإجراءات والضوابط في جميع الأوقات، متناسبة مع المخاطر التي حددها الموظفون من خلال التقييم الذي يجرى بموجب الفقرة 3–2–2، ومستجيبة لها.

4–2–3 الاستعراض يجب أن يجري الموظفون استعراضًا دوريًا للتدابير الأمنية التي طبقوها بموجب الفقرة 4–2–2 أعلاه، وأن يقوموا بتحديثها حسب الاقتضاء.

4–2–4 استخدام موارد تكنولوجيا المعلومات والاتصالات يجب إدارة جميع نظم تكنولوجيا المعلومات والاتصالات، بما في ذلك نظم المعلومات الإدارية، المستخدمة لمعالجة أو تخزين البيانات التي تقع ضمن نطاق هذه السياسة، بالامتثال للقسم 505 من دليل التعليمات الإدارية وأي أحكام أخرى ذات صلة من دليل التعليمات الإدارية.

4–2–5 التخزين يجب تخزين البيانات في أماكن مناسبة وبطريقة تحميها من المعالجة العرضية أو غير المصرّح لها، أو الفقدان أو التلف، مع أخذ مستوى السرّية في الاعتبار. وإذا كانت البيانات ستعالج أو تخزّن من جانب مقدم لخدمات النظم السحابية، تنطبق استراتيجية منظمة الأغذية والزراعة الخاصة باعتماد نُظم الحوسبة السحابية والخطوط التوجيهية وعملية تقييم المخاطر الخاصة بالحوسبة السحابية.

4-2-6 الوصول إلى البيانات

لا يجوز السماح بالوصول إلى البيانات ومنح هذه الإمكانية إلا للأشخاص الذين يحتاجون إلى الاطلاع على البيانات لتحقيق الغرض من معالجتها، وذلك بحسب مستوى السرّية المنسوب إليها. ويجب حفظ سجل بأسماء الأشخاص المصرّح لهم وبحقوق الوصول التي تم منحها.

ويجب أن يتأكد الموظفون، قبل نقل البيانات إلى أطراف ثالثة لغرض معالجتها، من أن التدابير الأمنية التي تطبقها هذه الأطراف مشابهة على الأقل للتدابير المطلوب تطبيقها على البيانات ذات مستوى السرّية نفسه في المنظمة.

5- الشفافية

"نحن واضحون ومنفتحون حيال البيانات التي نعالجها، والسبب وراء معالجتها، والطريقة التي نستخدمها فيها. ويمكننا أن نفسّر ذلك بصورة واضحة لمزودي البيانات"

5-1 النقاط الرئيسية

يعني مبدأ الشفافية التحلي بالوضوح والانفتاح مع مزودي البيانات لدى جمع البيانات، أي تحديد *"ما هي"* البيانات التي تعتزم المنظمة معالجتها، و*"لماذا"* يتطلب الأمر معالجة هذه البيانات، و*"كيف"* ستتم معالجتها. ويتباين مستوى المعلومات التي يتم توفيرها تبعًا لطبيعة البيانات والسياق التشغيلي.

5-2 المسؤوليات

5-2-1 الموجبات العامة

يكون الموظفون مسؤولين عن توفير معلومات كافية وذات صلة ومحدّثة بشأن معالجة البيانات، حسب الاقتضاء، إلى مزود البيانات، بما يشمل إمكانية تقديم مزوّدي البيانات لطلبات تتعلق ببيناتهم على النحو المبيّن في الفقرة 33 أدناه.

5-2-3 الأدوات التي تعزز الشفافية

يجب استخدام الأدوات المناسبة، مثل المذكرات الإعلامية، لإطلاع مزود البيانات على عملية معالجة بياناته طيلة دورة حياة هذه البيانات. ويجب استعراض هذه الأدوات بشكل منتظم لضمان بقاء المعلومات المقدمة إلى مزود الخدمات ذات صلة ومحدّثة.

5-2-5 الاستثناءات

يجب استشارة وحدة حماية البيانات في حال لم يتم توفير المعلومات. ويجب تسجيل أسباب عدم توفير المعلومات، بالكامل واستعراضها بصورة منتظمة للتأكد من أن الظروف الداعمة لقرار عدم توفير المعلومات لم تتغيّر.[18]

[18] مثلًا في حالات الطوارئ الناجمة عن القيود الأمنية واللوجستية، قد لا يكون من الممكن توفير المعلومات بشكل فوري إلى مزودي البيانات لدى جمع البيانات.

رابعًا– تصنيف البيانات ومستويات السرّية

12- يكون الموظفون مسؤولين عن تصنيف البيانات على أساس محتواها، وحساسيتها، والمخاطر المتصلة بالإفصاح عنها بشكل غير الملائم.

13- وهناك أربعة مستويات من السرّية يعكس كلّ منها حساسية البيانات التي يعالجها الموظفون والمخاطر ذات الصلة التي يمكن أن تنشأ عن استخدامها أو الإفصاح عنها بطريقة غير مصرّح لها.

14- ويجب أن تصنّف البيانات ضمن أحد مستويات السرّية الأربعة التالية:

مستوى السرّية	الوصف والتعرّض للمخاطر	الأمثلة
البيانات العامة	بيانات غير حساسة بما أن المنظمة قد وافقت على إتاحتها للجمهور العريض.[19] المخاطر: **لا يوجد** ليس من المتوقع بشكل معقول أن يُلحق الوصول غير المصرّح له إلى البيانات أو الإفصاح غير الملائم عنها، الضرر بالمنظمة أو بمزود البيانات.	• التقارير المنشورة أو الإحصاءات أو البيانات الصحفية.
البيانات الداخلية	بيانات لا يجوز الإفصاح عنها خارج المنظمة بسبب طابعها التحضيري أو غير المكتمل، أو بسبب الحاجة إلى موافقة داخلية. المخاطر: **متوسطة** يمكن التوقع بصورة معقولة أن يُلحق الوصول غير المصرّح له إلى البيانات أو الإفصاح غير الملائم عنها، الضرر بمزود البيانات أو بالمنظمة (مثل تقويض عمليات اتخاذ القرارات المستقلة في المنظمة، على سبيل المثال لا الحصر).	• الاتصالات الداخلية. • وثائق المشاريع، والتقارير السردية والمالية للمشاريع حيث قد يكون هناك حاجة إلى موافقة مزود البيانات على نشر هذه المعلومات. • مسودة الوثائق الفنية التي هي قيد الإعداد والتي لا تزال بحاجة إلى المصادقة عليها والموافقة على نشرها للعموم.

[19] تجوز إتاحة البيانات العامة مجانًا للجمهور وفقًا لسياسة المنظمة بشأن النفاذ المفتوح وأحكام البيانات المفتوحة الأخرى المتعلّقة بقواعد البيانات الإحصائية.

مستوى السرّية	الوصف والتعرّض للمخاطر	الأمثلة
البيانات السرّية	بيانات حساسة بطبيعتها. المخاطر: **عالية** يُلحق الوصول غير المصرّح له إلى البيانات أو الإفصاح غير الملائم عنها، ضررًا كبيرًا بمزود البيانات أو بالمنظمة. ويمكن أن يكون الضرر اللاحق بالمنظمة ضررًا ذا طابع مالي أو قانوني أو استراتيجي أو تشغيلي أو متعلّق بالسمعة.	• المعلومات بشأن المساعدة الفنية المقدمة إلى بلدان محددة واتفاقات المانحين مع الأعضاء. • البيانات المتناهية الدقة التي يحدد مزود البيانات أنه لا يجب الإفصاح عنها. • قوائم المشاركين في الدورات التدريبية التي تنظمها المنظمة والوثائق الأخرى التي تتضمن بيانات شخصية مثل الأسماء، وعنوان البريد الإلكتروني، والألقاب الوظيفية، وأرقام الهاتف. • ممارسة العناية الواجبة وتقييم المخاطر. • عمليات اختيار الموظفين.
البيانات الحساسة	بيانات حساسة جدًا بطبيعتها. ويمكنها أن تشمل أيضًا البيانات التي تصبح مصنّفة على أنها حساسة والتي يجب تصنيفها على هذا النحو بسبب محتواها أو الظروف المحيطة بتوليدها أو نقلها. المخاطر: **عالية جدًا** يُلحق الوصول غير المصرّح له إلى البيانات أو الإفصاح غير الملائم عنها، ضررًا جسيمًا للغاية بمزود البيانات أو بالمنظمة. وقد يكون الضرر الملحق بالمنظمة ضررًا جسيمًا ولا يمكن إصلاحه وله طابع مالي أو قانوني أو استراتيجي أو تشغيلي أو متعلّق بالسمعة.	• البيانات الشخصية التي تكشف عن عرق الأفراد، أو إثنيتهم، أو دينهم، أو صحتهم، أو بياناتهم الوراثية، أو مقاييسهم الحيوية، من جملة أمور أخرى. • الوثائق المتعلّقة بالتحقيقات أو الإجراءات التأديبية أو إجراءات الاستئناف. • الوثائق التي يحيلها الأعضاء أو الأطراف الثالثة إلى المنظمة شرط المحافظة على سرّيتها. • الوثائق المتعلّقة بالمشتريات والتي يشير البائع إلى أنها تحتوي على معلومات حساسة تجاريًا.

15- ولا يجوز الإفصاح عن البيانات لأي طرف خارجي أو للجمهور إلا باتباع إجراءات التصريح أو النشر المعمول بها.

16- وعندما يتم تطبيق تدابير وضوابط أمنية محددة، يجب أن يقرر الموظفون بحسب كل حالة على حدة، مستوى الحماية التي يجب تقديمها للبيانات التي يعالجونها في ضوء المخاطر التي تم تحديدها في نوع معيّن من عمليات المعالجة. ويجب أن يتخذ الموظفون التدابير الأمنية الملائمة التي تتناسب مع مستوى السرّية المحدد وتستجيب له.

17- وفي حال حدد مزود البيانات مستوى سرّية بياناته قبل نقلها إلى المنظمة، فيجب على موظفي هذه الأخيرة أن يعالجوا هذه البيانات وفقًا لمستوى السرّية ذاك. وفي حال لم يكن مزود البيانات قد حدد مستوى السرّية بعد، تصنّف البيانات على أنها سرّية إلا إذا اتفقت المنظمة ومزود البيانات على خلاف ذلك.

18- ولضمان مستوى من الحماية يتناسب مع مستوى السرّية ويستجيب له، على الموظفين مراجعة مستوى التصنيف بشكل منتظم وتعديله عند الاقتضاء. وفي حال لم يقم موظفو المنظمة أو مزود البيانات بإسناد مستوى السرّية للبيانات، تصنّف الأخيرة على أنها سرّية.

19- وفي حال وجود أي شكّ أو عدم يقين بشأن مستوى السرّية، على الموظفين استشارة رؤساء مكاتبهم، أو ممثل المنظمة أو المدير العام المساعد/ الممثل الإقليمي، أو وحدة حماية البيانات، حسب الاقتضاء، لالتماس التوجيهات.

خامسًا- واجب الحفاظ على السرّية

20- يجب توخي أقصى درجات التكتم عند معالجة البيانات طيلة دورة حياتها. ويخضع الموظفون للمساءلة عند معالجة البيانات، بما في ذلك عند نقلها إلى طرف ثالث. كما أنهم ملزمون بواجب الحفاظ على سرّية البيانات. وقد أنشئ هذا الواجب عملاً بالمادة 301-1-5 من النظام الأساسي للموظفين، والفقرة 39 من معايير السلوك لموظفي الخدمة المدنية الدولية، والفقرة 5-12 من مدونة السلوك الأخلاقي للمنظمة، وينطبق على جميع الموظفين. وقد يخضع الموظفون الذين لا يتقيّدون بهذه الأحكام عند التعامل مع معلومات داخلية أو سرّية أو حسّاسة اطلعوا عليها بحكم وظيفتهم الرسمية، لإجراءات تأديبية أو إدارية أخرى.

21- ويجب أن يكفل الموظفون سرّية البيانات التي يجمعونها أو يصلون إليها أو يعالجونها. ولا يجوز الوصول إلى البيانات أو نقلها إلا لتحقيق الغرض من معالجتها، ولا يجب الإفصاح عنها لأي شخص آخر، بما في ذلك لطرف ثالث أو لموظفين آخرين في المنظمة، إلا إذا نالت الجهة المتلقية إذنًا صريحًا بالوصول إلى البيانات أو بالحصول عليها رهنًا بتدابير أمنية تناسب مستوى سرّيتها.

سادسًا- التطبيق المحدد للمبادئ الخمسة لحماية البيانات

توفير المعلومات لمزودي البيانات

22- يجب توفير الحد الأدنى التالي من المعلومات لمزود البيانات، قبل جمع البيانات أو في غضون فترة زمنية معقولة من جمعها: (1) البيانات التي ستتم معالجتها؛ (2) والغرض من معالجتها؛ (3) وما إذا كان سيتم نقلها إلى طرف ثالث؛ (4) وكيفية طلب الوصول إليها أو التحقق منها أو تصحيحها أو حذفها أو الاعتراض على استخدامها؛ (5) وكيفية تقديم

شكوى [إلى وحدة حماية البيانات] بشأنها في حال عدم رضى مزود البيانات مثلًا بالرد على طلبه السابق؛ (6) وهوية جهة الاتصال المعنية بالاستفسارات أو الطلبات الخاصة بالبيانات في المنظمة، وتفاصيل الاتصال بهذه الجهة.

23- وعندما تتم معالجة بيانات شخصية، يجب توفير المعلومات لمزود البيانات بلغة واضحة ومفهومة وبصيغة تلائم عمره، ومدى إلمامه بالقراءة والكتابة، وهشاشة وضعه.

معالجة البيانات الحساسة

24- **اعتماد التدابير المناسبة.** يجب تطبيق تدابير وضمانات محددة لكفالة حسن استخدام البيانات الحساسة وحمايتها، مع مراعاة سياق المعالجة والتشغيل والمبادئ الخمسة لحماية البيانات.

25- **تقييم الضرورة.** يجب أن يقوم الموظفون، قبل جمع البيانات الحساسة، باستكشاف إمكانية تحقيق الغرض من المعالجة من دون معالجة بيانات حساسة.

26- **الأسس الشرعية.** يجب أن تعالج البيانات في إطار الأنشطة المضطلع بها بموجب ولاية المنظمة وبما يتماشى مع إطارها القانوني. إضافة إلى ذلك، لا يجوز للموظفين معالجة البيانات الحساسة إلا بالاستناد إلى أحد الأسس الشرعية التالية التي تناسب الظروف السائدة: (1) الموافقة الصريحة لمزوّد البيانات؛ (2) أو حماية المصالح الحيوية لمزود البيانات.

27- **التوجيه.** تُلتمس توجيهات وحدة حماية البيانات في ما يتعلّق بالإجراءات المناسبة التي يجب اتخاذها، حسب الاقتضاء، عند معالجة بيانات حساسة يكون من المرجح أن تنجم عنها مخاطر عالية على مزودي البيانات والمنظمة.

نقل البيانات

28- **البيانات التي تحصل عليها المنظمة.** يجب أن يكفل الموظفون أن البيانات التي تحصل عليها المنظمة قد نقلت إليها بالاستناد إلى الأسس الشرعية المناسبة، مثل موافقة مزود البيانات.

29- **البيانات التي تنقلها المنظمة إلى طرف ثالث.** لا يجوز أن ينقل الموظفون البيانات إلى طرف ثالث إلا بشرط أن يقدم هذا الأخير مستوى من حماية البيانات مطابقًا أو مشابهًا لمستويات الحماية التي تقدمها قواعد المنظمة وسياساتها، بما في ذلك هذه السياسة.

30- **تقييم الحماية التي يقدمها الطرف الثالث.** يجب أن يقيّم الموظفون مستوى الحماية التي يقدمها الطرف الثالث تبعًا لمستوى سرّية البيانات، قبل نقل هذه البيانات إليه. ويتطلب ذلك إجراء تقييم للضمانات الأمنية الفنية والتنظيمية التي يقدمها الطرف الثالث، وللمخاطر والمنافع التي ينطوي عليها نقل البيانات، ولأية عناصر أخرى ذات صلة بعملية النقل. وإذا تقرر، بالتشاور مع وحدة حماية البيانات، حسب الاقتضاء، أن الطرف الثالث عاجز عن تقديم مستوى من الحماية مطابق أو مشابه لما تقدمه التدابير التي تطبقها المنظمة على البيانات، فإنه يجب تحديد التدابير المناسبة للتخفيف من المخاطر المحتملة أو عدم نقل البيانات.

31- **الترتيبات التعاقدية.** تنقل البيانات بناء على ترتيب تعاقدي خطي أو، حسب الاقتضاء، بإدراج الضمانات ذات الصلة في الترتيبات التعاقدية المبرمة بموجب القواعد والخطوط التوجيهية المعمول بها لكل نوع من أنواع الترتيبات، مثل الأقسام 501 و507 و701 من دليل التعليمات الإدارية، واستراتيجية المنظمة لإشراك القطاع الخاص (قائمة غير شاملة).

ويجوز أن يكون هناك استثناءات محدودة لاشتراطات الصكوك التعاقدية، ولكن يجب أن تكون هذه الاستثناءات معقولة في الظروف القائمة وأن يتم تسجيل مبرراتها، بما في ذلك التدابير الحمائية المتخذة.

32- **وسائل نقل البيانات**. لا يجوز نقل البيانات إلا بالوسائل التي تكفل حمايتها الملائمة. ويجب أن تحدد وسائل نقل البيانات بالاستناد إلى مستوى سرّية هذه البيانات. وتماشيًا مع القسم 1-2-7 أعلاه، يجب أن يكفل الموظفون، بالتشاور مع وحدة حماية البيانات، حسب الاقتضاء، أن الطرف الثالث سيتلف البيانات المنقولة إليه أو سيعيدها إلى المنظمة ما أن يتحقق الغرض من نقلها.

طلبات مزودي البيانات

33- **نوع الطلبات**. يجب أن يكون مزود البيانات قادرًا على طلب الوصول إلى بياناته التي تعالجها المنظمة وتصحيحها وحذفها، أو على الاعتراض على معالجتها من جانب المنظمة.

(أ) الوصول. يجوز لمزود البيانات أن يطلب تأكيدًا على ما إذا كانت تجري معالجة بياناته، وفي هذه الحالة، أن يطلب الوصول إليها.

(ب) التصحيح. يجوز لمزود البيانات أن يطلب تصحيح بياناته أو تحديثها.

(ج) الحذف. يجوز لمزود البيانات أن يطلب حذف بياناته إذا (1) لم تعد البيانات ضرورية لتحقيق الغرض من معالجتها، (2) أو سحب مزود البيانات موافقته على معالجة البيانات ولم يكن هناك أي أساس شرعي آخر للمعالجة.

(د) الاعتراض. يجوز لمزود البيانات أن يعترض على معالجة بياناته لدى جمعها. ويجب أن يقوم موظفو المنظمة بإعلام مزود البيانات بما يمكن أن يترتب عن اعتراضه من تداعيات محتملة، حسب الاقتضاء.[20]

34- **التنفيذ**. يكفل الموظفون تلقي طلبات الحصول على البيانات وتصحيحها وحذفها والاعتراض على معالجتها، وتسجيل هذه الطلبات والتحقق منها ومناولتها والإجابة عليها في الوقت المناسب وبطريقة فعالة. وإذا توافرت الأسس الشرعية لتلبية الطلب، يجب أن يتخذ الموظفون الإجراءات المناسبة للاستجابة بصورة كاملة أو جزئية للطلب الوارد.

35- **القيود**. بعد استشارة وحدة حماية البيانات، يجوز رفض طلبات مزودي البيانات أو تقييدها على أساس (1) أمن وسلامة الموظفين أو الأطراف الثالثة أو مزودي البيانات، (2) أو القواعد والتوجيهات ذات الصلة المتعلّقة بالسرّية والإفصاح عن المعلومات، بما في ذلك هذه السياسة، (3) أو أن الطلب غير واضح أو غير معقول.

36- **أحكام خاصة**. لا تقيّد هذه السياسة حقوق مكتب المفتش العام بالوصول إلى أي بيانات تملكها المنظمة المنصوص عليها في ميثاقه. ولا تمنح هذه السياسة حقوقًا جديدة للوصول إلى البيانات التي يقوم مكتب المفتش العام، ومكتب الشؤون الأخلاقية، وأمين المظالم بإدارتها ومعالجتها.

[20] على سبيل المثال، إذا اعترض أحد المستفيدين من المنظمة على معالجة بياناته في سياق أنشطة التحويلات النقدية، على المنظمة الإحجام عن معالجة هذه البيانات. وإن لم يعد من الممكن أن تقدم المنظمة المساعدة من دون هذه البيانات، فسوف تحتاج إلى إعلام المستفيدين بذلك.

انتهاكات البيانات

37- يجب أن يقوم الموظفون الذين يعالجون البيانات، باستشارة رؤساء مكاتبهم، أو ممثل المنظمة أو المدير العام المساعد/ الممثل الإقليمي، حسب الاقتضاء، سرعان ما يتنبّهون لانتهاك بحق البيانات. ويجب تحديد ما إذا كان هذا الانتهاك يُسفر أم لا، عن خطر يهدد مزود البيانات أو المنظمة. ويجب تقييم الخطر الذي تم تحديده وحفظ سجل موجز بالتحليل الذي أجري وإبلاغ وحدة حماية البيانات به لكي تقدم مشورتها بشأن إجراءات التخفيف التي يمكن اتخاذها.

38- وعندما يسفر انتهاك البيانات عن خطر يهدد مزود البيانات، يتم إبلاغ هذا الأخير به وبالتدابير المطبقة للتخفيف منه إلا إذا قررت وحدة حماية البيانات أن التبليغ غير ضروري أو مناسب.

سابعًا– المسؤوليات والرقابة

لجنة الإشراف على حماية البيانات

39- تتولّى لجنة الإشراف على حماية البيانات، الرقابة على أنشطة حماية البيانات على نطاق المنظمة وترصد تنفيذ هذه السياسة. وتكون هذه اللجنة مسؤولة أمام المدير العام وترفع تقاريرها وتقدم مشورتها إليه في ما يتعلّق بمسائل حماية البيانات.

40- وتتألّف لجنة الإشراف على حماية البيانات من:

(أ) رئيس: نائب للمدير العام يعيّنه المدير العام.

(ب) وأعضاء: مدير شعبة خدمات تكنولوجيا المعلومات، والمستشار القانوني (مكتب الشؤون القانونية)، ومسؤول الشؤون الأخلاقية (مكتب الشؤون الأخلاقية)، ومدير شعبة الخدمات اللوجستية، ومدير شعبة إدارة الموارد البشرية، ومدير شعبة دعم المشاريع، وعضوين من المكاتب الميدانية يعيّنهما المدير العام.

41- وتقدم لجنة الإشراف على حماية البيانات التوجيهات على نطاق المنظمة لأنشطة حماية البيانات. وتقوم بما يلي:

(أ) رصد تفعيل هذه السياسة وتنفيذها والتوصية، حسب الاقتضاء، بتطوير صكوك إضافية؛

(ب) تلقي التقارير بشأن تنفيذ هذه السياسة والتوصية، حسب الاقتضاء، بإدخال تعديلات عليها؛

(ج) استعراض هذه السياسة مرّة واحدة كل ثلاث سنوات على الأقل مع مراعاة الدروس المستفادة من تنفيذها، وأي تغيّرات في الهياكل التنظيمية والسياسات التكميلية، وأي تطوّرات أخرى في منظمة الأغذية والزراعة أو منظومة الأمم المتحدة يكون من شأنها التأثير في تنفيذ هذه السياسة؛

(د) رفع تقارير دورية إلى المدير العام لتقديم المشورة إليه بشأن تفعيل هذه السياسة والصكوك ذات الصلة، وبشأن مدى ملاءمة التدابير المطبّقة.

42- وتجتمع اللجنة مرّتين على الأقل سنويًا، إما بشكل افتراضي وإما بحضور شخصي. وبناء على موافقة الأعضاء، يجوز للجنة أن تتخذ قراراتها عن طريق المراسلة.

43- وتحال المسائل المثارة في مجموعة تنسيق البيانات بقيادة رئيس الخبراء الاقتصاديين والتي يترتب عنها انعكاسات على حماية البيانات، إلى لجنة الإشراف على حماية البيانات لالتماس توجيهاتها.

وحدة حماية البيانات

44- تضطلع وحدة حماية البيانات بالأمور التالية:

(أ) توفير دعم الأمانة للجنة الإشراف على حماية البيانات؛

(ب) رصد الامتثال لهذه السياسة، ورفع تقارير منتظمة بشأن الامتثال لهذه السياسة أو تنفيذها وبشأن أي قضايا أخرى تتعلّق بحماية البيانات إلى لجنة الإشراف على حماية البيانات؛

(ج) إدارة طلبات مزودي البيانات وتقييمها؛

(د) إسداء المشورة إلى رؤساء المكاتب، أو المديرين العامين المساعدين/ الممثلين الإقليميين، والموظفين بشأن التدابير الرامية إلى كفالة الامتثال لهذه السياسة، بما في ذلك المنهجية التي يجب اتباعها لتقييم تأثير حماية البيانات، ولمعالجة البيانات الحساسة العالية المخاطر، ولتقييم صلاحية الطلبات التي يقدمها مزودو البيانات، وإسداء المشورة بشأن انتهاكات البيانات؛

(هـ) تلقي التقارير السنوية من رؤساء المكاتب، أو المديرين العامين المساعدين/ الممثلين الإقليميين، بشأن تنفيذ هذه السياسة بقدر ما يتعلّق الأمر بوحداتهم، حسب الاقتضاء.

رؤساء المكاتب والمديرون العامون المساعدون/ الممثلون الإقليميون

45- تقع على عاتق رؤساء المكاتب والمديرين العامين المساعدين/ الممثلين الإقليميين المسؤوليات التالية:

(أ) الإشراف على معالجة البيانات ضمن نطاق مسؤولياتهم؛

(ب) تأدية دور جهة الاتصال في ما يخص قضايا حماية البيانات التي تقع ضمن نطاق مسؤولياتهم؛

(ج) التماس مشورة لجنة الإشراف على حماية البيانات بشأن الاستفسارات المتعلّقة بتطبيق هذه السياسة وتفسيرها حسب الاقتضاء؛

(د) وضع إجراءات داخلية في الوحدة لكفالة معالجة البيانات وفقًا لهذه السياسة؛

(هـ) رصد أنشطة معالجة البيانات داخل الوحدة لكفالة الامتثال لهذه السياسة، وتحديد المخاطر المحتملة والتدابير الكفيلة بالتخفيف منها؛

(و) إسناد مسؤوليات محددة داخل الوحدة على المستوى الفردي لمناولة البيانات، مع مراعاة الحاجة إلى الفصل بين المهام بشكل صحيح خلال دورة حياة البيانات؛

(ز) رفع التقارير السنوية بشأن تنفيذ هذه السياسة والصكوك ذات الصلة إلى وحدة حماية البيانات.

الموظفون

46- يكون جميع الموظفين مسؤولين بصفة فردية عن الامتثال لهذه السياسة وللصكوك ذات الصلة. ويعني ذلك من جملة أمور أخرى، أن الموظفين مطالبون بالقيام بما يلي:

(أ) تحديد الغرض من معالجة البيانات ووسائلها وفقًا لهذه السياسة؛

(ب) تنفيذ التدابير الفنية والتنظيمية المناسبة التي يمكنها أن تشمل إبرام الصكوك التعاقدية المناسبة، من أجل ضمان أن تُعالجَ البيانات وفقًا لهذه السياسة، واستعراض هذه التدابير بشكل منتظم وتحديثها عند الاقتضاء؛

(ج) حفظ سجلات ملائمة لعمليات معالجة البيانات، واتفاقات تقاسم البيانات، وطلبات مزودي البيانات وشكاواهم، وتقييمات تأثير حماية البيانات، والإخطارات بانتهاك البيانات، وطلبات مزودي البيانات والمسائل ذات الصلة؛

(د) إعلام رؤسائهم على الفور في حال حدوث انتهاكات للبيانات والتعاون في أي تحقيق كان بشأن انتهاك مشبوه للبيانات؛

(هـ) التماس مشورة وحدة حماية البيانات في ما يتعلّق بتطبيق هذه السياسة وتفسيرها.

ثامنًا– الاستعراض والتعديل

47- سيتم استعراض هذه السياسة من جانب لجنة الإشراف على حماية البيانات بعد 12 شهرًا من إصدارها، وسيتم تعديلها حسب الاقتضاء. وبعد ذلك، ستستعرض هذه السياسة مرّة واحدة كل سنتين على الأقل بهدف ضمان بقائها ملائمة للغرض المنشود منها.

48- وتصبح أي تعديلات يتم إدخالها على هذه السياسة نافذة اعتبارًا من تاريخ نشرها.

تاسعًا– تاريخ بدء النفاذ

49- يكون هذا التعميم الإداري نافذًا بصورة فورية ويحل محل التعميمين الإداريين رقم 23/2013 بشأن سياسة السرية ورقم 01/2021 بشأن مبادئ حماية البيانات الشخصية اللذين يتم سحبهما.

الملحق الأول

التعاريف

البيانات المجهولة المصدر تعني المعلومات التي لا ترتبط بشخص طبيعي محدد أو يمكن التعرّف عليه، أو البيانات الشخصية التي تم تجهيل مصدرها لكي يتعذر التعرّف على مزودها.

الموافقة تعني الإشارة الحرة والمحددة والمستنيرة والتي لا لبس فيها إلى رضى مزود البيانات على معالجة بياناته، والتي يمكن أن تكون ضمنية، أو صريحة عندما يتعلّق الأمر بالبيانات الحساسة.

البيانات تعني أي معلومات صالحة للمعالجة وتكون آتية من المنظمة أو أفصح مزود البيانات عنها للمنظمة. وتشمل البيانات بموجب هذه السياسة، البيانات الشخصية وغير الشخصية الواردة بأي شكل كان.

انتهاك البيانات يعني فقدان البيانات، بما في ذلك البيانات الحساسة، أو إتلافها أو تعديلها أو الوصول إليها أو الحصول عليها بشكل عرضي أو غير مصرّح له، أو أي استخدام آخر لها لأغراض غير مصرّح لها، ما يقوّض سرّية هذه البيانات أو أمنها أو توافرها أو سلامتها.

دورة حياة البيانات تعني جميع المراحل في حياة البيانات، من التخطيط والجمع والمعالجة والتخزين والنقل وصولًا إلى الإتلاف.

مزود البيانات هو شخص اعتباري أو فرد يُفصح عن البيانات للمنظمة. وبموجب هذه السياسة، يجوز للأشخاص الاعتباريين، بما في ذلك أعضاء المنظمة، والمنظمات التابعة لمنظومة الأمم المتحدة، والمنظمات الحكومية الدولية، والمنظمات غير الحكومية، وكيانات القطاع الخاص، أن يفصحوا عما لديهم من بيانات شخصية أو غير شخصية متعلّقة بفرد معيّن للمنظمة.

التشفير هو عملية تحويل البيانات لجعلها غير قابلة للقراءة من دون امتلاك معرفة خاصة من قبيل "مفتاح" أو كلمة مرور.

البيانات غير الشخصية تعني أي معلومات ذات طابع مالي أو فني أو تشغيلي لا يكون لها صلة بفرد معروف الهوية أو يمكن التعرّف عليه. وتشمل البيانات غير الشخصية على سبيل المثال، التقارير المالية أو بيانات البائع الحساسة تجاريًا أو البيانات التي تتضمن معلومات حساسة أمنيًا قام الأعضاء بالإفصاح عنها.

البيانات الشخصية تعني أي معلومات ذات صلة بفرد معروف الهوية أو يمكن التعرّف عليه، مثل الأسماء، وعناوين مكان العمل والسكن، بما في ذلك عنوان البريد الإلكتروني، وتاريخ الولادة، والألقاب الوظيفية، إلخ.

يشير مصطلح **الموظفين**، على النحو المستخدم في هذه السياسة، إلى موظفي المنظمة والهيئات التابعة لها، بما في ذلك الاستشاريين، والمشتركين في اتفاقيات الخدمات الشخصية، وموظفي المشاريع الوطنيين، والمتطوعين، والمتدربين، وجميع الأفراد الآخرين الذين يقدمون خدمات للمنظمة بموجب اتفاق تعاقدي.

معالجة البيانات تعني أي عملية أو مجموعة عمليات، مؤتمتة أم لا، تجرى على البيانات وتشمل على سبيل المثال لا الحصر التجميع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكييف أو التغيير أو الاسترجاع أو التشاور أو الاستخدام أو النقل (سواء أكان ذلك بواسطة الحاسوب أم شفويًا أم خطيًا) أو النشر، وإلا الإتاحة أو التصحيح أو الإتلاف.

استخدام الأسماء المستعارة يعني معالجة البيانات بحيث لا يعود من الممكن نسبها إلى مزود بيانات محدد من دون استخدام معلومات إضافية. ويجب الاحتفاظ بمثل هذه المعلومات الإضافية بشكل منفصل وهي تخضع لتدابير فنية من أجل كفالة عدم إمكانية نسب البيانات الشخصية إلى فرد معيّن.

البيانات الحساسة تعني البيانات التي يصنّفها الموظفون على أنها حساسة استنادًا إلى احتمال ظهور مخاطر محتملة نتيجة الإفصاح غير الملائم عنها وإلى ما لذلك من تأثير. وتشمل هذه البيانات على سبيل المثال لا الحصر، البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني، والآراء السياسية، والمعتقدات الدينية، فضلًا عن البيانات الوراثية أو المتعلّقة بالمقاييس الحيوية والبيانات الصحية للأفراد والتي تعتبر تلقائيًا حساسة جدًا. كما أنها تشمل البيانات غير الشخصية ذات الطابع الحساس تجاريًا أو اقتصاديًا والتي ترتبط بالأمن القومي، أو المعلومات الأخرى ذات القدر نفسه من الحساسية التي يوفرها أعضاء المنظمة أو أشخاص اعتباريين آخرين.

الطرف الثالث يعني أي كيان، غير المنظمة ومزود البيانات، تُنقل البيانات إليه.

الملحق الثاني

أمثلة على كيفية تطبيق المبادئ الخمسة لحماية البيانات

المبدأ	المثل
النزاهة	تعتزم المنظمة، في سياق مشروع لمَنح المستفيدين، استخدام البيانات الشخصية الواردة في طلبات الحصول على المنح لإرسال طلبات استقصائية. وتماشيًا مع مبدأ النزاهة، يوصى بالمبادرة أولا إلى التماس الموافقة عن علم من أصحاب البيانات على استخدام بياناتهم الشخصية لمثل هذا الغرض. وبعد وقوع كارثة طبيعية، تبقى الاتصالات والوصول إلى بلد عضو معيّن متضررة بشدة. وبما أنه لا يمكن تحديد نوع المساعدة المطلوبة فور وقوع الكارثة أو بعدها، تجري المنظمة عملية جمع واسعة للبيانات بغرض تقييم احتياجات الأشخاص المتضررين. وبعد انتهاء حالة الطوارئ، تحذف المنظمة البيانات غير الضرورية لتقديم المساعدة الفنية التي تم تحديدها. وعند إعداد اقتراح تمويل من جهات مانحة متعددة الأطراف، تجمع المنظمة مجموعة واسعة من البيانات، بما في ذلك البيانات الواردة من الشركاء في المشروع. وتماشيًا مع مبدأ النزاهة، يحتفظ المكتب القطري لفترة محددة فقط بالبيانات بعد تصنيفها. وعندما يتعذّر تحديد مدة الاحتفاظ بالبيانات، يحدد المكتب فترة احتفاظ أولية تخضع لاستعراض دوري. وإذا تم تقاسم البيانات مع طرف ثالث، تُتخذ إجراءات معقولة لضمان قيام هذا الطرف بحذف البيانات.
السلامة	تعتزم المنظمة تنفيذ مشروع تحويلات نقدية بالاستناد إلى بيانات تسجيل المستفيدين التي تم جمعها قبل 12 شهرًا من بدء المشروع. ولضمان دقّة البيانات، يجب التحقق قبل تنفيذ المشروع مما إذا كانت مواقع المستفيدين وتركيبة الأسر المعيشية قد تغيّرت خلال هذه الفترة. ويجب الاضطلاع بصورة دورية، وإلى حين انتهاء المشروع، بعمليات فحص للبيانات للتحقق من دقتها.
المسؤولية	يقوم مكتب إقليمي بمعالجة البيانات لأنشطة عديدة مثل تنفيذ المشاريع، والتوظيف، والتعاقد مع البائعين، وعقد حلقات العمل. ولإثبات الامتثال لهذه السياسة، يحفظ المكتب سجلات محدّثة لكل نشاط من أنشطة معالجة البيانات ويحدد في كل منها الغرض من المعالجة، ونوع البيانات المستخدمة، والجهة المتلقية للبيانات (إن وجدت)، والحدود الزمنية للاحتفاظ بالبيانات، والتدابير الأمنية.
الأمن	وضعت المنظمة بروتوكولًا يتعلّق بالأنشطة البحثية كجزء من إطار برنامج الإدارة المستدامة للحياة البرية. وتماشيًا مع مبدأ الأمن، ينصّ البروتوكول على الحاجة إلى نسب بيانات تعريفية (*SubjectID*) متمايزة للأفراد بما يضمن فصل البيانات – من خلال إتاحة الوصول إلى البيانات للمحققين الأساسيين فقط – وتشفير الملفات التي تتضمن بيانات شخصية وحمايتها بواسطة كلمة مرور.

	وفي سياق عقود التنبيهات الأمنية التي ترسل بموجبها الجهة المتعاقدة مع المنظمة تنبيهات إلى موظفي هذه الأخيرة على هواتفهم الشخصية لتحذيرهم أو إبقائهم على بيّنة من الأوضاع التي قد تمثّل خطرًا، يُحظر صراحة استخدام هذا النوع من البيانات لأغراض تسويقية من جانب الجهة المتعاقدة أو تقاسمه مع أطراف ثالثة. إضافة إلى ذلك، يجرى تقييم لمستوى الحماية التي تقدمها الجهة المتعاقدة قبل نقل البيانات إليها.
الشفافية	يجري مكتب قطري تابع للمنظمة مناقشات مع البلد المضيف بهدف إتاحة اللقاحات ضد كوفيد-19 للموظفين ولمن يستحقّ من الأشخاص الذين يعيلونهم. وتماشيًا مع مبدأ الشفافية، يتم إطلاع الموظفين عبر استبيان محدد على إفصاح البيانات الشخصية ذات الصلة للسلطات الوطنية المعنية بالرعاية الصحية لغرض إعطاء اللقاح، فيوافقون عليه. وتتلقى المنظمة بيانات البحوث من اتحاد شريك. وتحتاج المنظمة إلى إطلاع الشريك على البيانات التي ستتم معالجتها، وكيف سيتم ذلك، ومع من سيتم تقاسمها، والمدة الزمنية التي يتوقع أن تستغرقها عملية المعالجة. وعند معالجة طلب يقدمه الشريك للوصول إلى البيانات، يجب أن يحرص الموظفون على حصولهم على الوثائق المثبتة لهوية مقدم الطلب وعلى عدم الكشف عن أي بيانات تتعلّق بالأطراف الثالثة.