

## سياسة الاتحاد الدولي بشأن حماية البيانات الشخصية

تصریح بإصدار الوثيقة				
صاحب الشأن	الاسم	المنصب	التوقيع	تاريخ الاعتماد
المؤلف	James De France	كبير المستشارين القانونيين		
المؤلف	Lucie Laplante	المستشارة القانونية العامة		
صاحب الوثيقة	Elhadj As Sy	الأمين العام		
صرح بإصدار الوثيقة	Julie Hall	رئيسة الموظفين ومديرة مكتب الأمين العام		
	Anitta Underlin	وكيلة الأمين العام المعنية بالشؤون الإدارية		
	Jagan Chapagain	وكيل الأمين العام المعني بالبرامج والعمليات		
المشاركون	Dr. Jemilah Mahmood	وكيلة الأمين العام المعنية بالشركات ومديرة قسم الشركات وتنمية الموارد بالنيابة		
	Andrew Rizk	مدير قسم الشؤون المالية والإدارية		
	Katherine Hummel	مديرة قسم الموارد البشرية بالنيابة		
	Sylvia Gil	مديرة قسم تكنولوجيا المعلومات		
	Pascale Meige	مديرة قسم منع الكوارث والأزمات والتصدي لها والتعافي منها		
	Derk Segaar	مدير قسم الاتصالات		
	Emmanuel Capobianco	مدير قسم الصحة والرعاية		
	Cecile Aptel	مديرة وحدة السياسات والاستراتيجيات والمعارف		
	Anthony Garnett	مدير مكتب التدقيق الداخلي والتحقق		



## مراقبة التعديلات

تخضع هذه الوثيقة لإجراءات مراقبة التعديلات وستسجل أدناه أي تعديلات تُدخل على النسخ الأصلية.

## تاريخ إجراء التعديلات

النسخة	التاريخ	ملاحظات
1.0	٢٥ مارس ٢٠١٩	

## تنبيه

قد لا تكون النسخة الورقية من هذه الوثيقة أحدث نسخة متاحة. وبوسعكم الاطلاع على أحدث نسخة، تسود على كل النسخ السابقة، على شبكة FedNet.

## المحتويات

- ١- مقدمة ٣
- ١-١ تعليقات استهلاكية ٣
- ٢-١ نطاق التطبيق ٣
- ٣-١ تعاريف ٣
- ٢- مبادئ عامة بشأن حماية البيانات
- ١-٢ النزاهة والشرعية
- ٢-٢ المعلومات
- ٣-٢ تحديد الغرض
- ٤-٢ جودة البيانات والتقليل منها
- ٥-٢ الاحتفاظ بالبيانات والتخلص منها
- ٦-٢ السرية والأمن
- ٣- حقوق أصحاب البيانات
- ١-٣ الاطلاع على البيانات الشخصية وتصحيحها والاعتراض على معالجتها وحذفها
- ١-١-٣ معلومات عن المعالجة
- ٢-١-٣ الاطلاع على البيانات الشخصية وتصحيحها
- ٣-١-٣ الاعتراض على المعالجة
- ٤-١-٣ طلب الحذف
- ٢-٣ إجراءات الطلبات المتعلقة بالبيانات الشخصية
- ٣-٣ الرد على الطلبات
- ٤- الالتزامات
- ١-٤ تحليل أثر حماية البيانات
- ٢-٤ انتهاك البيانات
- ١-٢-٤ الإخطار عن انتهاك البيانات الشخصية
- ٢-٢-٤ إخطار صاحب البيانات عن انتهاك البيانات الشخصية
- ٣-٤ المساءلة
- ١-٣-٤ الأدوار والمسؤوليات
- ٢-٣-٤ الوثائق
- ٥- عمليات نقل البيانات الشخصية
- ١-٥ نقل البيانات إلى أطراف ثالثة
- ٢-٥ نقل البيانات إلى هيئات التحقيق أو السلطات الحكومية
- ٦- بيانات الاتصال

## أولاً- مقدمة

### ١-١ تعليقات استهلاكية

يجمع الاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر (المشار إليه فيما يلي باسم "الاتحاد الدولي") ويعالج كميات هائلة من البيانات الشخصية من خلال الأنشطة الكثيرة التي يضطلع بها. وتكتسي حماية البيانات الشخصية أهمية بالغة للاتحاد الدولي، ولذلك فقد وضع سياسة عامة بشأن حماية البيانات الشخصية ("السياسة"). وتسعى هذه السياسة إلى حماية حق الأفراد في الخصوصية، مع ضمان قدرة الاتحاد على جمع البيانات الشخصية واستخدامها في إطار أدائه لمهمته.

وترتبط حماية البيانات الشخصية بالسياق؛ ولا يمكن تغطية كل ما قد ينشأ من سيناريوهات. ولهذا السبب، تبين هذه السياسة أفضل الممارسات العالية المستوى، على غرار الأدوات الدولية الرائدة لحماية البيانات.

ويدرك الاتحاد الدولي أن مجرد وضع سياسة عامة لا يشكل إجراءً كافياً لضمان الحماية من المخاطر الناجمة عن إساءة استخدام البيانات الشخصية أو فقدانها. وسيوفر الاتحاد، في إطار التنسيق مع هذه السياسة، التدريب والمعلومات والبيانات في مجال حماية البيانات، وسيواصل مراجعته الجارية للإجراءات والسياسات الداخلية ذات الصلة وتنفيذه المستمر لها.

ويحظى الاتحاد الدولي بامتيازات وحصانات في العديد من البلدان التي يعمل فيها. وعلى الرغم من أن تطبيق هذه السياسة لا يمس أيًا من الامتيازات والحصانات التي يتمتع بها الاتحاد الدولي، فإنه ينبغي مراعاة القوانين والنظم القانونية السائدة في البلدان التي يعمل فيها الاتحاد عند تقييم المخاطر التي يتعرض لها الأفراد و/أو الجماعات والمرتبطة بحماية البيانات.

### ٢-١ نطاق التطبيق

تطبق المبادئ الواردة في هذه السياسة على معالجة البيانات الشخصية. ولا تطبق السياسة على المعلومات المجهولة المصدر، أي المعلومات التي لا يمكن ربطها بشخص طبيعي محدد الهوية أو يمكن تحديد هويته.

ويؤزم بالامتثال لهذه السياسة أي شخص يعمل في خدمة الاتحاد الدولية، بما في ذلك، على سبيل المثال لا الحصر، الموظفون والموظفون المتعاقدون والموظفون المحليون والمندوبون والموظفون المعارون. ويُنْتَظَر أيضاً من المتدربين والمتطوعين والمستشارين الالتزام بالمبادئ والممارسات الواردة في السياسة.

وعلى الرغم من أن هذه السياسة تهدف أساساً إلى حماية البيانات الشخصية، فإن البيانات غير الشخصية المتعلقة بالجماعات، من قبيل المعتقدات السياسية أو الدينية، يمكن أن تعرض مجموعات من الأفراد للخطر. ولذلك ينبغي استخدام المبادئ الواردة في هذه السياسة كدليل عند جمع المعلومات المتعلقة بالجماعات أو معالجتها.

### ٣-١ تعاريف

لأغراض هذه السياسة، تنطبق التعاريف التالية على ما يلي:

#### حماية البيانات

تعني حماية البيانات، في سياق هذه السياسة، مجموعة من المبادئ والممارسات المطبقة لضمان أن تكون جميع البيانات الشخصية التي يجمعها ويستخدمها الاتحاد الدولي أو تجمع وتستخدم بالنيابة عنه بيانات دقيقة ومفيدة، وألا تكون البيانات الشخصية عرضة لسوء الاستخدام أو الضياع أو التلف، وألا يجري الاطلاع عليها وتبادلها دون ترخيص.

## البيانات الشخصية

البيانات الشخصية هي كل معلومة يمكن أن تؤدي إلى التعرف على شخص طبيعي حي (محدد الهوية أو يمكن تحديد هويته). وتشمل بعض أمثلة البيانات الشخصية الاسم، والبريد الإلكتروني أو البيانات التي تحدد الموقع، ورقم الهوية، والنوع الاجتماعي، والوضع العائلي، وتاريخ ومكان الميلاد.

## البيانات الشخصية الحساسة

تعتبر أنواع البيانات الشخصية الحساسة، بما فيها، على سبيل المثال لا الحصر، المعلومات المتعلقة بالصحة والمعتقدات الدينية والسياسية والبيانات البيومترية والجينية، أصناف خاصة من البيانات الشخصية. وتجدر الإشارة إلى أن تحديد ما إذا كانت البيانات الشخصية حساسة أم لا قد يتوقف إلى حد بعيد على السياق.

وينبغي وضع تدابير حماية وقيود إضافية أثناء عمليتي الجمع والمعالجة إذا تبين أن البيانات الشخصية المتاحة حساسة. وقد تتضمن تدابير الحماية الإضافية هذه، على سبيل المثال لا الحصر، الضوابط المحددة لتناول المعلومات السرية للغاية في المبادئ التوجيهية المتعلقة بمعالجة المعلومات.

## مراقب البيانات

يُستخدم مصطلح "مراقب البيانات" للإشارة إلى الشخص أو الكيان الذي يحدد أغراض ووسائل معالجة البيانات الشخصية. وتقع على عاتق مراقب البيانات المسؤولية الرئيسية عن حماية البيانات الشخصية.

وقد يكون هناك أكثر من مراقب واحد للبيانات في الممارسة العملية. وتجدر الإشارة أيضًا إلى أنه قد تنشأ ظروف يكون فيها مراقب البيانات طرفاً ثالثاً، ولن يضطلع الاتحاد حينها سوى بمهمة معالجة البيانات الشخصية.

## معالج البيانات

المعالج هو الشخص أو الكيان الذي ينجز عملية معالجة واحدة أو أكثر للبيانات الشخصية بناءً على تعليمات يصدرها مراقب البيانات.

## الطرف الثالث

الطرف الثالث هو أي شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو هيئة أخرى غير صاحب البيانات أو الاتحاد أو مراقب البيانات أو معالج البيانات.

## معالجة البيانات الشخصية

هو أي عملية، أو مجموعة من العمليات، الآلية أو غير الآلية، التي تطبق على البيانات الشخصية، بما في ذلك، على سبيل المثال لا الحصر، الجمع والتسجيل والتخزين أو التكيف أو التغيير والاسترداد والاستخدام والنقل والتعميم والتصحيح أو الإلتلاف.

## صاحب البيانات

هو الشخص الذي تخضع بياناته الشخصية للمعالجة.

## الأشخاص المتضررون

هم الأشخاص الذين يلتمسون حماية الاتحاد الدولي أو مساعدته أو يستفيدون من حماية الاتحاد أو مساعدته. وقد يشمل هذا التعريف أي شخص في البلد أو المجتمع المحلي الذي يعمل فيه الاتحاد الدولي.

## الموظف المعني بحماية البيانات

هو موظف يعمل لدى الاتحاد الدولي ويشرف على تنفيذ هذه السياسة.

## انتهاك البيانات الشخصية

هو الاطلاع غير المرخص به على بيانات شخصية أو التسبب في إتلافها أو فقدانها أو تغييرها أو الكشف عنها.

## ثانياً- المبادئ العامة

تسترشد عملية معالجة البيانات التي ينفذها الاتحاد بالمبادئ العامة التالية:

### ١-٢ النزاهة والشفافية

ينبغي معالجة البيانات الشخصية بطريقة نزيهة وشفافة. ويعني ذلك أن الاتحاد الدولي لن يعالج البيانات الشخصية إلا في حالة وجود أساس شرعي، وأن من الضروري تزويد أصحاب البيانات بمعلومات يمكن فهمها بسهولة وتتعلق بجمع بياناتهم ومعالجتها.

وتمثل الموافقة الأساس الشرعي المفضل لمعالجة المعلومات الشخصية. بيد أنه ينبغي، في حالة تعذر الحصول على موافقة حرة ومستنيرة تماماً، توثيق الظروف دوماً.

ويمكن، في ظل ظروف معينة، استخدام أساس واحد أو أكثر من الأسس الشرعية التالية، إضافة إلى الموافقة أو بديل عنها.

- تنفيذ عقد؛
- التقيد بالالتزام القانوني الذي يخضع له الاتحاد الدولي؛
- حماية المصالح الحيوية لأصحاب البيانات؛
- الاضطلاع بعمل من أجل النفع العام أو تماشياً مع المهمة الموكلة إلى الاتحاد الدولي؛
- السعي إلى تحقيق مصالح الاتحاد الدولي المشروعة.

وعند تقييم الأسس الشرعية التي تنطبق على عملية معالجة معينة، ينبغي إيلاء اعتبار خاص للمخاطر التي يتعرض لها صاحب البيانات (مثل الأطفال) وحساسية البيانات الشخصية التي يتعين جمعها ومعالجتها، مع ملاحظة أن ما يمكن اعتباره معلومات شخصية عادية في سياق ما قد يعتبر شديد الحساسية في سياق آخر.

### ٢-٢ المعلومات

ينبغي للاتحاد الدولي تزويد أصحاب البيانات بالمعلومات التالية، بطريقة يمكن فهمها بسهولة أثناء جمع البيانات الشخصية أو في أقرب وقت ممكن بعد ذلك:

- الأساس الشرعي الذي تستند إليه معالجة البيانات،
- الاستخدام المقصود للبيانات؛

- أهمية توفير معلومات دقيقة وكاملة واثابة أي تحديثات ذات صلة بالمعلومات التي سبق تقديمها؛
- الأطراف التي يمكن تبادل البيانات الشخصية معها ومكان إقامتها؛
- كيف ستخزن البيانات ومتى ستحذف وتحت أي ظرف يتم ذلك؛
- يجوز لأصحاب البيانات سحب موافقتهم حينما تكون الموافقة هي الأساس الشرعي الذي يُستند إليه في عملية المعالجة؛
- الجهات التي يمكن الاتصال بها في الاتحاد الدولي لطرح أي أسئلة بشأن استخدام البيانات الشخصية.

وقد لا تُقدّم المعلومات الواردة أعلاه حينما يكون الاتحاد الدولي على علم، أو حينما يمكنه الافتراض بصورة معقولة، بأن صاحب البيانات قد أتيح لها بالفعل إمكانية الحصول على المعلومات ذات الصلة أو أن بإمكانها الحصول على هذه المعلومات، وحينما يكون توفير هذه المعلومات خطوة غير عملية قياساً بالفوائد التي تعود على صاحب البيانات. وبالإضافة إلى ذلك، فقد لا تتاح المعلومات الواردة أعلاه حينما تكون مصلحة الاتحاد المشروعة في عدم الكشف عن هذه المعلومات أكبر من حقوق صاحب البيانات. ويمكن، في حالات الشك، استشارة الموظف المعني بحماية البيانات للحصول على توجيهات.

وبالإضافة إلى هذه السياسة، نشر الاتحاد الدولي بيانات بشأن الخصوصية على بعض مواقع الشبكة وفي اتصالات الإلكترونيّة أخرى. وثراجع بيانات الخصوصية هذه للحصول على معلومات أدق بشأن جمع البيانات الشخصية واستخدامها في سياق الموقع الشبكي ذي الصلة أو العملية ذات الصلة.

## ٣-٢ تحديد الغرض

ينبغي جمع البيانات الشخصية ومعالجتها لغرض محدد، ويجوز بوجه عام معالجتها لأغراض أخرى تتوافق مع الغرض الأصلي. ويجوز للاتحاد معالجة البيانات الشخصية لأغراض إضافية غير متوافقة مع هذا الغرض عند التأكد من وجود أساس شرعي وبعد النظر في حقوق أصحاب البيانات والموازنة بين هذه المعالجة الإضافية والمخاطر التي قد تنجم عنها.

## ٤-٢ جودة البيانات والتقليل منها

ينبغي أن تكون البيانات الشخصية التي يجري جمعها بيانات مناسبة ومفيدة ودقيقة وغير زائدة عن الحد المطلوب بالنظر إلى الغرض المحدد الذي تجمع من أجله البيانات. وينبغي، عند الضرورة، اتخاذ جميع التدابير المعقولة لضمان تحديث البيانات الشخصية. وينبغي، في حال اكتشاف بيانات شخصية غير دقيقة، تصحيح هذه البيانات أو حذفها دون تأخير لا مبرر له.

## ٥-٢ الاحتفاظ بالبيانات والتخلص منها

ينبغي ألا تتجاوز فترة الاحتفاظ بالبيانات الشخصية، سواء كانت مخزنة في شكل نسخ ورقية أو إلكترونياً، الوقت الضروري لتحقيق الغرض المحدد الذي تعالج من أجله. وينبغي لبوادر المكتبات والمحفوظات احترام الجداول الزمنية للاحتفاظ بالبيانات وينبغي لجميع المكاتب أو الأقسام أو الإدارات التابعة للاتحاد الدولي الالتزام بهذه الجداول الزمنية على أساس الاحتياجات المستمرة المتوقعة للبيانات الشخصية ذات الصلة ووفقاً لسياسة إدارة المعلومات والجداول الزمنية لتصنيف السجلات ذات الصلة والتخلص منها. ويمكن استشارة الموظف المعني بحماية البيانات للحصول على توجيهات فيما يتعلق بعملية الاحتفاظ بالبيانات.

وينبغي التخلص من البيانات الشخصية وفقاً للسياسة المعمول بها في الاتحاد الدولي (على سبيل المثال، سياسة تصنيف المعلومات والمبادئ التوجيهية المرافقة). وينبغي الرجوع إلى قسم تكنولوجيا المعلومات للحصول على المساعدة بشأن سبل التخلص من البيانات وحذف الملفات الإلكترونية بشكل آمن.

## ٦-٢ السرية والأمن

تنفذ جميع مراحل معالجة البيانات الشخصية بطريقة تكفل مستوى مناسباً من الأمن والسرية للبيانات الشخصية. ويتعين، على وجه التحديد، حفظ البيانات الشخصية بصورة آمنة وحمايتها من عمليات انتهاك البيانات.

ومن الأهمية بمكان مراجعة مدى كفاية جميع التدابير الأمنية المتخذة خلال مرحلة وضع المشاريع التي تتضمن معالجة البيانات الشخصية بما يكفل وجود ترتيبات أمنية كافية في جميع مراحل المشروع.

ويراجع الاتحاد الدولي، حسب الاقتضاء، التدابير الرامية إلى ضمان أمن البيانات ويحدثها حتى يكفل مستوى كافياً من الحماية للبيانات فيما يتعلق بدرجة حساسية البيانات الشخصية.

## ثالثاً- حقوق أصحاب البيانات

١-٣ وفقاً للنقطتين ٢-٣ و ٣-٣، يتمتع أصحاب البيانات بالحقوق التالية. وسيضمن الاتحاد توفير آلية رسمية تتيح لأصحاب البيانات إعمال حقوقهم عن طريق تقديم طلب في هذا الصدد.

### ١-٣-١ معلومات عن المعالجة

يجق لصاحب البيانات أن يطلب معرفة ما إذا كان الاتحاد الدولي قد عاج بياناته الشخصية أو هو بصدد معالجتها أو ينوي معالجتها . ويجق له كذلك معرفة الغرض المحدد (الأغراض المحددة) من معالجة بياناتها

### ٢-١-٣ الاطلاع على البيانات الشخصية وتصحيحها

يجق لصاحب البيانات مراجعة بياناته الشخصية للتأكد من مدى دقتها واكتمالها ووجاهتها. ولدى العثور على بيانات غير دقيقة أو غير مستوفاة، يصحح الاتحاد البيانات الشخصية ذات الصلة ويستكملها في حينه.

### ٣-١-٣ الاعتراض على المعالجة

يجق لصاحب البيانات أن يعترض في أي وقت من الأوقات على معالجة بياناته الشخصية. وحينما يكون هذا الاعتراض مبرراً، يتوقف الاتحاد عن معالجة البيانات الشخصية المعنية للغرض المتعلق (الأغراض المتعلقة) بهذا الاعتراض.

### ٤-١-٣ طلب الحذف

يجوز لصاحب البيانات أن يطلب إلى الاتحاد الدولي حذف بياناته الشخصية نهائياً. وينبغي للاتحاد، إذا تبين له وجود مبرر لهذا الطلب، التقيد بقواعد سياسة أمن المعلومات ذات الصلة لضمان إتلاف البيانات المطبوعة والإلكترونية على حد سواء.

### ٢-٣ الإجراءات الخاصة بالطلبات المتعلقة بالبيانات الشخصية

ينبغي، على قدر الإمكان، تقديم طلب إعمال أي من الحقوق المدرجة في النقطة ١-٣ كتابياً إلى الموظف المعني بحماية البيانات. ويجب أن يتضمن هذا الطلب شرحاً واضحاً لموضوع الطلب (على سبيل المثال، تحديد ما إذا كان الطلب من أجل التصحيح أو الاعتراض)، وأن يتضمن حججاً وأدلة كافية تسمح للاتحاد بتلبية هذا الطلب.

وقد تُطلب معلومات إضافية إذا كان الطلب غير واضح أو كانت المعلومات المقدمة غير وافية.



ويجب أن يكون أي طلب مصحوباً ببيانات الاتصال الخاصة بصاحب الطلب والمستندات الكافية التي تثبت أن الطرف الذي قدم الطلب هو صاحب البيانات أو ممثلها القانوني أو الوصي عليها. وقد يطلب تقديم وثائق إضافية إذا اعتبرت المستندات المقدمة غير كافية. ومن المستلم به أنه قد لا يكون بوسع الأشخاص المتأثرين التعامل مع الموظف المعني بحماية البيانات مباشرة. ولهذا السبب، ينبغي لموظفي الاتحاد الدولي أن ييسروا، حسب الاقتضاء، معالجة هذه الطلبات.

### ٣-٣ الرد على الطلبات

يتلقى صاحب البيانات (أو ممثله القانوني)، في كل الحالات، رداً في الوقت المناسب بطريقة يفهمها.

ومع ذلك، فهناك عدد من الحالات التي قد لا يحظى فيها الطلب بالقبول، ولا يقدم فيها سوى قدر محدود من الردود. ومن أمثلة هذه الحالات ما يلي:

- حينما تكون هناك أسباب تدعو إلى الاعتقاد بأن الطلب تعسفي أو قائم على الغش؛
- حينما يكون الطلب غير واضح، و/أو الحجج الواردة فيه لا تستند إلى حقائق؛
- حينما تؤدي الموافقة على الطلب إلى تعريض شخص أو أكثر للخطر؛
- حينما يثبت أن الامتثال للطلب خطوة مستحيلة أو غير ملائمة أو تستلزم جهداً غير متناسب لدى موازنتها مع حق صاحب البيانات؛
- حينما يتعارض الطلب مع احتياجات الاتحاد الدولي وأولوياته الميدانية المهيمنة في إطار سعيه إلى تحقيق مصالحه المشروعة؛
- حينما تكون معالجة البيانات الشخصية ضرورية لأغراض حفظ الوثائق أو الأغراض الإحصائية ذات النفع العام، من أجل حماية حرية التعبير؛
- حينما تكون معالجة البيانات الشخصية ضرورية للامتثال لالتزام قانوني ما أو لرفع دعوى قانونية أو ممارسة حق أو الدفاع عنه أمام القضاء..

### رابعاً- الالتزامات

#### ١-٤ تحليل أثر حماية البيانات

يُجري الاتحاد تحليلاً لأثر حماية البيانات حينما تؤدي عمليات معالجتها، على الأرجح، إلى تعريض حقوق أصحاب البيانات أو حرمتهم لمخاطر كبيرة. وسوف تُعدّ توجيهات إضافية بشأن الحالات التي يكون فيها تحليل أثر حماية البيانات ضروري وبشأن كيفية إدارته. وبوجه عام، ينبغي أن يتضمن تحليل أثر حماية البيانات وصفاً للمشروع أو النظام أو السياسة أو الترتيب المتعلق بمعالجة و/أو تبادل البيانات الشخصية؛ وتحليلاً للمخاطر ذات الصلة؛ والتدابير المقترحة أو القائمة بالفعل لحماية البيانات الشخصية وفقاً لهذه السياسة.

وفيما يلي أمثلة للسيناريوهات التي قد يجرى فيها تحليل أثر حماية البيانات، بالتنسيق مع الموظف المعني بحماية البيانات:

- استخدام تكنولوجيا جديدة لمعالجة البيانات الشخصية؛
- إمكانية أن يكون الأفراد محلاً لاتخاذ قرارات أو للتوصيف بشكل آلي؛
- اقتراح نقل البيانات الشخصية إلى طرف ثالث قد لا يكون بإمكانه كفالة الضمانات الكافية لحماية البيانات؛
- وجود أصناف خاصة من البيانات الشخصية، مثل الحالة الصحية أو الآراء الدينية أو السياسية؛
- توقع مراقبة جماعية أو جمع للبيانات أو تبادلها.

## ٢-٤ انتهاك البيانات

على الرغم من التزام الاتحاد الدولي بتوفير أفضل ما يمكن توفيره من أمن للبيانات فيما يتعلق بمخاطر انتهاك البيانات، فإن من غير الممكن ضمان أي تدبير أممي (تقنياً كان أو مادياً أو تنظيمياً) بنسبة ١٠٠٪ لمنع حدوث أي انتهاك. ولذلك، فليس من المهم فقط توفير الأمن الكافي، بل يتعين أيضاً اعتماد طريقة موثوق بها لاكتشاف أي اختراقات أمنية والتعامل معها على وجه السرعة.

### ١-٢-٤ إخطار الموظف المعني بحماية البيانات عن انتهاك البيانات الشخصية

في حالة حدوث انتهاك للبيانات الشخصية، يُبلغ قسم تكنولوجيا المعلومات أو الجهة المعنية التي اكتشفت الانتهاك، سواء كانت مكتباً أو دائرة أو وحدة أو كياناً أو شخصاً، دون تأخير لا مبرر له، الموظف المعني بحماية البيانات (وأي مدير معني تابع للاتحاد، على النحو المحدد في سياسة الاستخدام المقبول للمعلومات). وينبغي أن تقدم إلى الموظف المعني بحماية البيانات المعلومات التالية:

- كيف اكتشف الانتهاك ومتى كان ذلك؛
- طبيعة الانتهاك، وأصناف البيانات الشخصية المتأثرة، والعدد التقديري للجهات المعنية موضوع البيانات؛
- العواقب المحتملة المترتبة على انتهاك البيانات الشخصية؛
- التدابير المتخذة أو المقترحة اتخذها للتصدي للانتهاك.

وينبغي أيضاً إبلاغ قسم تكنولوجيا المعلومات وإشراكه على نحو وثيق في جميع المراحل وفي جميع التدابير المتخذة فيما يتعلق بأي انتهاك للبيانات الشخصية. ويُبلغ أيضاً قسم الإعلام والاتصالات في أقرب وقت ممكن عن أي انتهاك يحدث.

### ٢-٢-٤ إخطار صاحب البيانات عن انتهاك البيانات الشخصية

استناداً إلى مشاورات تجرى، عند الاقتضاء، مع الموظف المعني بحماية البيانات والجهة الأخرى ذات الصلة، سواء كانت مكتباً أو إدارة أو وحدة، يبذل الاتحاد، إذا ثبت أن انتهاك البيانات يشكل خطراً كبيراً على حقوق أصحاب البيانات أو حريتهم، كل الجهود المعقولة لإبلاغ أصحاب البيانات المتأثرين، بطبيعة الانتهاك والتدابير المتخذة للتصدي له.

## ٣-٤ المساءلة

الأمين العام مسؤول عن تنفيذ هذه السياسة.

### ١-٣-٤ الأدوار والمسؤوليات

بالإضافة إلى الأدوار المبينة أدناه، قد تُحدد أدوار أخرى و/أو تقدم توجيهات أكثر تفصيلاً في إطار إجراءات وتوجيهات عمل تُعدّ في المستقبل.

#### المسؤولون الإداريون

المسؤولون الإداريون هم الجهة المسؤولة عن ضمان معرفة القوى العاملة التي يشرفون عليها للمبادئ المتعلقة بحماية البيانات المبينة في هذه السياسة والتعامل مع هذه البيانات وفقاً لهذه المبادئ. ويتحمل المسؤولون الإداريون أيضاً، عند الاقتضاء، مسؤولية تقديم الاستفسارات والشواغل المتعلقة بحماية البيانات إلى الموظف المعني بحماية هذه البيانات.

#### الموظف المعني بحماية البيانات

يعين الاتحاد الدولي موظفاً معني بحماية البيانات ويعمل كجهة تنسيق لجميع المسائل المتعلقة بحماية البيانات.

ويطلع الموظف المعني بحماية البيانات بالمسؤوليات الرئيسية التالية:

- تقديم توجيهات بشأن تطبيق هذه السياسة وتفسيرها؛
- تقديم المشورة بشأن الامتثال لهذه السياسة وتقديم توصيات بشأن سياسات الاتحاد أو ممارساته ذات الصلة أو تحديثها، عند الاقتضاء؛
- مساعدة مكاتب الاتحاد والإدارات والوحدات التابعة له في معالجة المسائل المتعلقة بوضع المشاريع التي تستعالج البيانات الشخصية بغية النظر في أي مخاطر (تقييم أثر حماية البيانات)؛
- العمل على ضمان مراعاة حماية البيانات في جميع مراحل المشروع (حماية البيانات بشكل مدروس وعلى نحو تلقائي)؛
- مراجعة الاتفاقات المتصلة بالبيانات الشخصية وتقديم المشورة بشأن المسائل المتعلقة بحماية البيانات بوجه عام.

ويمكن للموظف المعني بحماية البيانات أن يتشاور، عند الاقتضاء، مع أي من الجهات المشاركة ذات الصلة فيما يتعلق بتنفيذ هذه السياسة. ويتضمن هؤلاء المشاركون، على سبيل المثال لا الحصر، أمين المظالم، وقسم تكنولوجيا المعلومات، والمستشارة القانونية العامة.

#### المستشارة القانونية العامة

تتولى المستشار القانونية العامة مسؤولية إدارة المخاطر القانونية بالاتحاد فيما يتعلق بحماية البيانات وضمان توافق الالتزامات التي تعهد بها الاتحاد مع السياسة.

#### قسم تكنولوجيا المعلومات

يتولى قسم تكنولوجيا المعلومات المسؤولية العامة عن الحفاظ على موارد تكنولوجيا المعلومات بالاتحاد وضمان أمنها.

#### ٤-٣-٢ الوثائق

من أجل إثبات الامتثال للسياسة، ينبغي الاحتفاظ بسجلات مفصلة ودقيقة عن أنشطة جمع البيانات الشخصية ومعالجتها.

### خامساً- عمليات نقل البيانات الشخصية

تشكل عمليات نقل البيانات، سواء أكانت تتعلق بنقل بيانات الموظفين إلى مقدم خدمة كشوف المرتبات أو تبادل معلومات مفصلة عن الأشخاص المتضررين مع الشركاء في المساعدة النقدية، جزءاً عادياً وضرورياً من أداء الاتحاد الدولي ومن المساعدة التي يقدمها في جميع أنحاء العالم. ومع ذلك، ترافق كل عملية نقل للبيانات مخاطر تنجم عن إساءة استخدام البيانات أو الكشف عنها دون ترخيص.

#### ١-٥ عمليات نقل البيانات إلى أطراف ثالثة

ينبغي مراجعة جميع العمليات المقترحة لنقل البيانات الشخصية إلى أطراف ثالثة لضمان توافيقها مع المبادئ العامة المبينة في القسم الثاني من هذه السياسة. وبالإضافة إلى ذلك، لا ينبغي أن تنفذ عمليات نقل البيانات الشخصية إلى أطراف ثالثة إلا بعد أن يقدم الطرف الثالث ضمانات كافية لحماية البيانات وبعد إبرام اتفاق كتابي.

وكحد أدنى، تقتضي اتفاقيات نقل البيانات الكتابية من الطرف الثالث التقيد بما يلي:

- استخدام البيانات الشخصية المنقولة للغرض المحدد (الأغراض المحددة) في العقد ذي الصلة فقط، وبوجه عام وفقاً لتعليمات الاتحاد الدولي فقط؛
- إعادة البيانات الشخصية المنقولة إلى الاتحاد و/أو إتلافها، على النحو المنصوص عليه، عند انتهاء توفير الخدمات أو في أي وقت بناءً على طلب الاتحاد الدولي، على سبيل المثال من أجل الاستجابة لطلب صاحب البيانات بحذف بياناته الشخصية؛

- توفير ضمانات أمنية كافية لمنع أي تبديل أو ضياع أو اطلاق غير مرخص به للبيانات الشخصية (ينبغي أن تشمل هذه الضمانات، حسب الاقتضاء، القيود المفروضة على إمكانية الاطلاع، وتشفير البيانات المخزونة وأثناء النقل، والتخزين الآمن، والتدابير الأخرى)؛
- عدم تنفيذ أي عملية من عمليات نقل البيانات إلى أطراف ثالثة أخرى ما لم يوافق الاتحاد الدولي صراحةً على ذلك؛
- التعاقد من الباطن فقط بموافقة الاتحاد الدولي؛
- إخطار الاتحاد الدولي على الفور في حالة وقوع حادث أمني (انتهاك).

وفي ضوء تنوع السياقات السياسية والقانونية التي يعمل فيها الاتحاد الدولي، ينبغي إيلاء اهتمام خاص للإطار القانوني وقابلية إنفاذ الاتفاقات/العقود الكتابية في المنطقة (المناطق) ذات الصلة.

وأخيراً، فمن المسلم به أنه قد لا يكون من الممكن إبرام اتفاق كتابي قبل تبادل البيانات الشخصية مع شركاء معينين وفي ظروف طارئة معينة، مثل حالات الطوارئ الإنسانية. وينبغي أن تتخذ، في ظل هذه الظروف وحينما تكون عمليات نقل البيانات ضرورية لحماية المصالح الحيوية للأشخاص المتأثرين، جميع التدابير اللازمة في أقرب وقت ممكن بعد حالة الطوارئ، لحماية البيانات المنقولة، بما في ذلك السعي إلى إبرام اتفاق كتابي.

## ٢-٥ عمليات النقل إلى هيئات التحقيق أو السلطات الحكومية

يجوز للاتحاد الدولي، في ظل ظروف معينة، نقل البيانات الشخصية إلى هيئات تحقيق معينة أو إلى سلطة حكومية ما، بما فيها وكالات إنفاذ القانون والمحاكم. وقد تُنفَّذ عمليات النقل هذه بناءً على طلب أو مبادرة خاصة من الاتحاد الدولي.

ولا يجوز للاتحاد الدولي التعاون بشأن هذا الطلب ونقل البيانات الشخصية إلا إذا وافق الطرف المتلقي على الشروط المنصوص عليها في النقطة ١-٥ واستوفيت الشروط التالية:

- يتلقى الاتحاد الدولي طلباً حكومياً يرد عبر القنوات الرسمية ويعتبره صحيحاً من الناحية القانونية، أو يكون الاتحاد قد أبرم اتفاقاً كتابياً مع الطرف الذي يقدم الطلب؛
- يكون نقل البيانات ضرورياً لأغراض الكشف عن وقوع جريمة جنائية أو انتهاك القواعد واللوائح التنظيمية للاتحاد الدولي أو منع ذلك أو التحقيق فيه أو محاكمة مرتكبيه؛
- يمكن أن يساعد نقل البيانات الطرف الطالب في مسعاه إلى تحقيق هذه الأغراض بدرجة كبيرة؛
- يقتصر نقل البيانات على البيانات الشخصية الضرورية للغاية لتحقيق الغرض؛
- لا يتعارض نقل البيانات على نحو غير متناسب مع الحقوق الأساسية للفرد.

يُستشار الموظف المعني بحماية البيانات قبل إبرام أي اتفاق لنقل البيانات الشخصية وفقاً لهذه النقطة.

## سادساً- بيانات الاتصال

يرجى إرسال أي أسئلة بشأن هذه السياسة أو بشأن تنفيذها إلى عنوان البريد الإلكتروني التالي: [dataprotection@ifrc.org]