UNHCR
المفوضية السامية للأمم المتحدة
لشؤون اللاجئين

سياسة

بشأن حماية البيانات الشخصية للأشخاص المعنيين باهتمام المفوضية السامية للأمم المتحدة لشؤون اللاجئين (المفوضية)

سياسة حماية البيانات

المحتويات

١
الأحكام العامة

1.1 الغرض

تضع هذه السياسة القواعد والمبادئ التي تتعلّق بمعالجة البيانات الشخصية للأشخاص المعنيين. ويتمثّل الغرض من هذه السياسة في ضمان قيام المفوضية بمعالجة البيانات الشخصية بطريقة تتوافق مع المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المُحوسبة[1] والصادرة عن الجمعية العامة للأمم المتحدة للعام 1990، ومع الصكوك الدولية الأُخرى التي تتعلّق بحماية البيانات الشخصية وخصوصية الأفراد. وسوف تُستَكمل هذه السياسة بمبادئ توجيهية تنفيذية توفّر التوجيه بشأن تنفيذها ومراقبتها والمساءلة بشأنها.

1.2 الأساس المنطقي

1.2.1 سعياً من المفوضية إلى أداء ولايتها المتمثلة في توفير الحماية والحلول على المستوى الدولي، وأيضًا عندما تعرض على الدول تقديم مساعيها الحميدة، تكون المفوضية، في أغلب الأحيان، مطالبة بتجهيز ومعالجة البيانات الشخصية للأشخاص المعنيين. ولربما تتضمن هذه المطالبةُ الحاجةَ إلى التشارك في البيانات الشخصية مع الشركاء المنفّذين و / أو الأطراف الثالثة. وتكمُن في عملية تجهيز ومعالجة البيانات الشخصية مخاطرُ متأصّلة، مثل فقدان البيانات، أو الإفصاح عنها إما عن طريق الخطأ أو دون ترخيص بذلك. وبأخذ الوضع المُستضعَف، على وجه الخصوص، لهؤلاء الأشخاص المعنيين، فإنّ طبيعة بياناتهم الشخصية تتّصف بطابع حسَّاس عمومًا؛ الأمر الذي يتطلّب من المفوضية بالتالي توخّي الحذر في التعامل مع تلك البيانات، بما يتماشى مع هذه السياسة. وبالنسبة إلى المفوضية، فإن الحماية الملائمة للبيانات الشخصية، بناءً على ذلك، تحظى بأهمية خاصة، وتضطّلع المفوضية بمسؤولية معالجة هذه البيانات بطريقة تحترم مبادئ حماية البيانات.[2]

1 الجمعية العامة للأمم المتحدة، المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المحوسبة، حسبما أُقرَّت بالقرار رقم 95/A/Res/45، بتاريخ 14 كانون الأول / ديسمبر 1990، وهي متوافرة على الرابط الإلكتروني التالي: http://www.refworld.org/docid/3ddcafaac.html.

2 اللجنة التنفيذية لبرنامج المفوض السامي للأمم المتحدة لشؤون اللاجئين أشارت إلى مبادئ حماية البيانات في الاستنتاجات التالية: رقم 91 (f) 2001 – (LII) متوافر على الرابط الإلكتروني: http://www.unhcr.org/3bd3e1d44.html؛ ورقم 93 (VIII) (b) 2002 – (LIII) متوافر على الرابط الإلكتروني: http://www.unhcr.org/3dafdd344.html؛ ورقم 102 (V) 2005 – (LVI)، متوافر على الرابط الإلكتروني: http://www.unhcr.org/43575ce3e.html.

1.2.2 تَستكمل هذه السياسة أيضًا أحكام النظام الأساسي للموظفين رقم 1-2 (أ) والالتزامات الواردة في مدونة قواعد السلوك الخاصة بالمفوضية، وعلى وجه الخصوص، المبدأ 6، الذي يُطالب الموظفين بصون المعلومات التي يتسنّى لهم الوصول إليها، والاستفادة منها بطريقة مسؤولة.

1.3 النطاق

1.3.1 تنطبق هذه السياسة على جميع البيانات الشخصية التي تحتفظ بها المفوضية فيما يتعلّق بالأشخاص المعنيين.[3] ولا تندرج عملية معالجة البيانات الأخرى، على سبيل المثال، البيانات المجمَّعة أو المجهولة المصدر، ضمن نطاق هذه السياسة، ولكنها مغطّاة، من جُملة أمور أُخرى، بسياسة المفوضية لتصنيف المعلومات، والتعامل معها والإفصاح عنها.

1.3.2 تنطبق هذه السياسة سواءٌ أكانت معالجة البيانات تأخذ مجراها داخل أحد مكاتب المفوضية، أم فيما بين مكاتب المفوضية المختلفة في البلد نفسه أو في أكثر من بلد واحد، أو سواءٌ أكانت البيانات الشخصية مُحوَّلة إلى شركاء تنفيذيين أم إلى الأطراف الثالثة. ويستمرّ تطبيق هذه السياسة حتّى بعد أن لم يعودوا هؤلاء الأشخاص محل اهتمام المفوضية.

1.3.3 الامتثال لهذه السياسة مُلزِم لجميع موظفي المفوضية.

3 المفوضية السامية للأمم المتحدة لشؤون اللاجئين، مذكرة بشأن ولاية المفوض السامي لشؤون اللاجئين ومكتبه، تشرين الأول/أكتوبر 2013، متوافرة على الرابط الإلكتروني http://www.refworld.org/docid/5268c9474.html.

1.4 الأحكام والتعاريف

تعتبر التعاريف التالية واجبة التطبيق تحقيقًا لأغراض هذه السياسة:

الموافقة

أي إشارة مستنيرة يعطيها صاحب البيانات بكامل حريته تدل على موافقته على معالجة بياناته الشخصية، وتُعطى هذه الموافقة خطّيًا أو شفويًا، أو عن طريق إجراء توكيدي واضح.

مراقب البيانات

هو أحد موظفي المفوضية، وفي العادة يكون هذا الموظف هو ممثّل المفوضية في المكتب القُطري، الذي يملك الصلاحية للإشراف على إدارة عملية معالجة البيانات الشخصية، وتحديد الغرض منها.

معالج البيانات

هو أحد موظفي المفوضية أو أي شخص طبيعي آخر أو منظمة، بمن في ذلك الشريك المنفّذ أو الطرف الثالث الذي ينفّذ عملية معالجة البيانات الشخصية بالنيابة عن مراقب البيانات.

مسؤول التنسيق بشأن حماية البيانات

من حيث المبدأ، هو موظف الحماية الأقدم لدى المفوضية العامل في أحد مكاتبها القطرية أو إحدى عملياتها، والذي يساعد مراقب البيانات في تنفيذ مسؤولياته بشأن هذه السياسة.

تقييم أثر حماية البيانات

أداة وعملية لتقييم آثار الحماية على أصحاب البيانات أثناء معالجة بياناتهم الشخصية، وفي تحديد الإجراءات العلاجية حسب الضرورة، لأجل تجنُّب هذه الآثار أو التقليل منها إلى الحد الأدنى.

الموظف المسؤول عن حماية البيانات

هو موظف تابع لشعبة الحماية الدولية في المقر الرئيسي للمفوضية، والذي يُشرف على تحقيق الامتثال لهذه السياسة، ورصد تطبيقها والإبلاغ عنها. أما مسؤوليات الموظف المسؤول عن حماية البيانات فهي محددة في الفقرة 3-7 من هذه السياسة.

صاحب البيانات

هو الشخص الذي تخضع بياناته للمعالجة.

اتفاقية تحويل البيانات

الاتفاقية المُبرمة بين المفوضية والشريك المنفّذ أو الطرف الثالث، والتي تنص على أحكام وشروط استعمال البيانات الشخصية، بما في ذلك تحديد مكوّنات البيانات التي ينبغي التشارك فيها، وأُسلوب تحويلها، والطريقة التي يجوز بوساطتها استخدام البيانات، وتدابير أمن البيانات، والمسائل الأُخرى ذات العلاقة.

الشريك المنفّذ

هو أي منظمة تُعيَّن ككيان مُستقل عن المفوضية، ويتشارك مع المفوضية من خلال اتفاقية شراكة في مشروع معيّن ليتولّى تنفيذ أنشطة برامجية ضمن إطار ولاية المفوضية.

البيانات الشخصية

هي أي بيانات ذات علاقة بأي شخص يمكن تحديد هويته من واقع تلك البيانات، أو من واقع تلك البيانات ومعلومات أُخرى، أو بأي وسيلة من المحتمل استخدامها بطريقة معقولة فيما يتعلق بتلك البيانات. وتشمل البيانات الشخصية بيانات السّيرة الذاتية، مثل الاسم، والجنس، والحالة الاجتماعية، وتاريخ ومكان الولادة، وبلد المنشأ، وبلد اللجوء، ورقم التسجيل الشخصي، والمهنة، والدين، والعرق، وبيانات السمات الحيوية (البيانات البيومترية)[4]، مثل الصورة الشخصية، وبصمات الأصابع، وصورة الوجه أو قزحية العين، وكذلك تشمل أي تعبير عن الرأي بشأن ذلك الشخص، مثل تقييم الحالة و / أو الاحتياجات المحددة.

خرق البيانات الشخصية

هو أي خرق لأمن البيانات، إما بشكل عَرَضي أو غير قانوني / غير مشروع، يؤدي إلى إتلاف البيانات الشخصية المنقولة، أو المخزّنة، أو المُعالجة، أو فقدانها، أو تغييرها، أو الكشف غير المصرّح به عنها، أو الوصول إليها.

4 البيانات البيومترية هي الخصائص البيولوجية (التشريحية أو الفسيولوجية) أو السلوكية، التي يُمكن استخدامها لتحديد هوية شخص ما عن طريق مقارنتها بالبيانات المرجعية المُخزَّنة لدى المفوضية.


© UNHCR / Dalia Khamissy

الشخص المعني

هو الشخص الذي تكون حمايته واحتياجاته للمساعدة موضع اهتمام المفوضية. ويشمل الأشخاص من هذا القبيل اللاجئين، وطالبي اللجوء، والأشخاص عديمي الجنسية، والأشخاص النازحين داخليًّا والعائدين.

معالجة البيانات الشخصية

هي أي عملية، أو مجموعة عمليات، سواءٌ أكانت آليةً أم غير آلية، تُجرى للبيانات الشخصية، وتشمل، على سبيل المثال لا الحصر، جمع البيانات، وتسجيلها، وتنظيمها، وهيكلتها، وتخزينها، وتكييفها أو تغييرها، واسترجاعها، والتشاور بشأنها، واستخدامها، وتحويلها (سواءٌ أكان ذلك بشكل محوسب، أو شفهي، أو خطي)، أو نشرها، أو توفيرها، أو تصحيحها، أو إتلافها.

الطرف الثالث

هو أي شخص طبيعي أو قانوني غير صاحب البيانات، أو المفوضية أو الشريك المنفّذ. ومن الأمثلة على الأطراف الثالثة: الحكومات الوطنية، أو المنظمات الدولية الحكومية أو غير الحكومية، أو كيانات القطاع الخاص، أو الأفراد.

٢
المبادئ الأساسية

2.1 المبادئ الأساسية لمعالجة البيانات الشخصية

يتعيَّن على كوادر المفوضية احترام وتطبيق المبادئ الأساسية التالية عند معالجة البيانات الشخصية:

(أ) المعالجة بطريقة مشروعة وعادلة
(ب) تحديد الغرض
(ت) الضرورة والتناسبية
(ث) الدقة
(ج) احترام حقوق صاحب البيانات
(ح) السّرّية
(خ) الأمن
(د) المساءلة والمراقبة

2.2 المعالجة بطريقة مشروعة وعادلة

يمكن معالجة البيانات الشخصية فقط إذا كانت المعالجة تُنفذ على أساس مشروع، وبطريقة عادلة تتّصف بالشفافية. كما يمكن للمفوضية معالجة البيانات الشخصية فقط على أساس واحد أو أكثر من المبادئ التالية:

(أ) الحصول على موافقة صاحب البيانات.
(ب) أن تصبّ معالجتها في تحقيق المصالح الحيوية أو الفُضلى لصاحب البيانات.
(ت) تمكين المفوضية من أداء ولايتها.
(ث) وفيما يتعدى ولاية المفوضية، تجوز معالجة البيانات الشخصية لكفالة سلامة وأمن الأشخاص المعنيين والأفراد الآخرين.

2.3 تحديد الغرض

يتعيَّن جمع البيانات الشخصية لغرض واحد أو أكثر من الأغراض المحددة والمشروعة، مع ضرورة عدم معالجتها بطريقة غير متوافقة مع هذا الغرض (تلك الأغراض).

2.4 الضرورة والتناسبية

ينبغي لعملية معالجة البيانات الشخصية أن تكون ضرورية ومتناسبة مع الأغراض التي تُعالج لأجلها. وبناءً على ذلك، يجب أن تكون تلك البيانات كافية وملائمة للغرض المحدد لها، وألّا تتجاوز ذلك الغرض.

2.5 الدقة

يجب أن تُسجَّل البيانات الشخصية بأقصى قدر ممكن من الدقة، وأن تُحدَّث حيثما تقتضي الضرورة، لضمان استيفائها للأغراض التي تُعالج لأجلها.

2.6 احترام حقوق صاحب البيانات

يتناول القسم 3 من هذه السياسة حقوق صاحب البيانات في الحصول على المعلومات، والوصول إليها، وتصحيحها، وحذفها والاعتراض عليها والتعامل معها.

2.7 السرية

يَتعيَّن على كوادر المفوضية المحافظة على سرّية البيانات الشخصية للأشخاص المعنيين في جميع الأوقات، حتى بعد أن لم يعد الشخص محل اهتمام المفوضية.

2.8 الأمن

لكي يتسنّى ضمان سرّية وسلامة البيانات الشخصية، يتعين وضع تدابير فنية وتنظيمية لأمن البيانات موضع التنفيذ، علمًا بأن القسم 4 من هذه السياسة يتعامل مع أمن البيانات والمسائل الأخرى ذات العلاقة. أما تحويل البيانات الشخصية إلى الأطراف الثالثة فهو مقتصرٌ على استيفاء الشروط المحددة في القسم 6 منها.

2.9 المساءلة والمراقبة

لأجل ضمان تحقيق المساءلة عن معالجة البيانات الشخصية بما يتوافق مع هذه السياسة، سوف تُنشئ المفوضية هيكلًا للمساءلة والمراقبة، حسبما يُحدده القسم 4 من هذه السياسة.

٣
حقوق صاحب البيانات

3.1 المعلومات

عندما تكون المفوضية بصدد جمع البيانات الشخصية، من الضروري أن تُخبر المفوضيةُ، خطيًّا أو شفهيًّا، صاحب البيانات بما يلي بطريقة ولغة يفهمها صاحب البيانات:

(أ) الغرض الأساسي (الأغراض الأساسية) الذي لأجله تُعالج البيانات الشخصية أو فئات منها.

(ب) إبلاغ صاحب البيانات بحقيقة ما إذا كانت البيانات التي تُعالج سوف تُحوَّل إلى الشريك المنفّذ (الشركاء المنفّذين)، أو إلى الأطراف الثالثة، في الحالات التي يكون فيها الشريك المنفّذ قائماً على جمع البيانات بالنيابة عن المفوضية.

(ت) أهمية قيام صاحب البيانات بتقديم بيانات دقيقة وكاملة.

(ث) واجب صاحب البيانات في الاستمرار في إطلاع المفوضية، و / أو – حسب الاقتضاء – الشريك المنفّذ بأي تغييرات تطرأ على حالته الشخصية.[5]

(ج) أي عواقب تترتّب على رفض تقديم، أو الإخفاق في تقديم البيانات الشخصية المطلوبة.

(ح) حق صاحب البيانات في طلب الحصول على بياناته الشخصية، أو تصحيحها أو حذفها.

(خ) حق صاحب البيانات في الاعتراض على جمع البيانات الشخصية.

(د) كيفية تقديم شكوى لدى مراقب البيانات، ولدى مكتب المفتّش العام.

5 على وجه الخصوص التغييرات التي تطرأ على أحواله المدنية، على سبيل المثال، واقعات الولادة، والوفاة، والزواج.

3.2 الحصول على:

يحق لصاحب البيانات، بناءً على طلبه، الحصول على ما يلي من المفوضية:

(أ) تأكيد بشأن ما إذا تمت أم لم تتم معالجة البيانات الشخصية الخاصة به، أو بأنها قيد المعالجة، أو بأنها ستتم معالجتها في المستقبل.
(ب)معلومات عن كلٍّ من البيانات الشخصية الجاري معالجتها، والغرض (الأغراض) من معالجة هذه البيانات، والشريك المنفذ (الشركاء المنفذين) و / أو الأطراف الثالثة التي حُوّلت هذه البيانات إليها، أو جاري تحويلها إليها، أو سوف يُصارُ إلى تحويلها إليها.

3.3 تصحيح وحذف المعلومات

3.3.1 يجوز لصاحب البيانات طلب تصحيح أو حذف البيانات الشخصية غير الدقيقة، أو غير المكتملة، أو غير الضرورية، أو الزائدة عن الحاجة.

3.3.2 في الحالات التي يطلب فيها صاحب البيانات تصحيح أو حذف بياناته الشخصية، ينبغي للمفوضية أن تطلب منه دليل إثبات يتعلّق بعدم دقة تلك المعلومات أو عدم اكتمالها.

3.4 الاعتراض

مع مراعاة نص الفقرة 3-7 أدناه، يجوز لصاحب البيانات الاعتراض على معالجة بياناته الشخصية في الحالات التي توجد فيها أسباب مشروعة تتعلّق بحالته الشخصية المحدّدة. فإذا كان الاعتراض مبررًا، يجب على المفوضية التوقف عن معالجة البيانات الشخصية المعنية.

3.5 طرائق تقديم الطلبات

3.5.1 يجوز لصاحب البيانات، أو لممثّله القانوني المفوّض، أو في حالة الأطفال، يجوز لأحد والدي الطفل أو لوصيه القانوني تقديم طلبات للحصول على معلومات حول كيفية الوصول إلى بياناتهم الشخصية، أو تصحيحها أو حذفها أو الاعتراض عليها. وينبغي أن تُقدَّم الطلبات شفهياً أو خطياً إلى مكتب المفوضية في البلد الذي تُعالج فيه البيانات.

3.5.2 قبل الامتثال لأي طلب أو اعتراض، ينبغي للمفوضية أن تتحقق من هوية الشخص المتقدم بالطلب أو الاعتراض. ويجب على المتقدّم بالطلب أن يثبت هويته بطريقة ملائمة. وفي حالة وجود ممثّل قانوني أو وصي قانوني، فلا بُدّ له من تقديم ما يثبت صلاحيته القانونية. وينبغي تقييم الطلبات والاعتراضات المُقدّمة من والدي الطفل أو أوصيائه من منظور المصلحة الفُضلى للطفل.

3.6 تسجيل الواقعة والاستجابة لها من قبل المفوضية

3.6.1 يجب على المفوضية تسجيل واقعة قيامها بتزويد صاحب البيانات بالمعلومات عملاً بنص الفقرة 3.1 من هذه السياسة، وكذلك تسجيل الطلبات التي تتلقّاها للحصول على المعلومات، أو تصحيحها، أو حذفها أو الاعتراض عليها، وردها على تلك الطلبات عملاً بنصوص الفقرات 3.2، 3.3 و3.4.

3.6.2 يتعيّن على المفوضية الاستجابة لأي طلب أو اعتراض، يُقدّم بمقتضى القسم 3 من هذه السياسة، خلال فترة زمنية معقولة، خطيًّا أو شفهيًّا، وبطريقة ولغة مفهومتين من جانب صاحب البيانات أو ممثله القانوني أو وصيّه القانوني، حسب الاقتضاء.

© UNHCR / M. Abu Asaker

3.7 القيود

استنادًا إلى المشاورات التي تُجرى مع مسؤول حماية البيانات، ومع الأطراف المعنية في المقر الرئيسي للمفوضية، يجوز للمفوضية رفض تقديم ردها على أي طلب أو اعتراض بمقتضى القسم 3 من هذه السياسة، أو تحديده أو تقييده إذا:

(أ) كان من شأن ذلك أن يشكل تدبيرًا ضروريًّا، أو متناسبًا لحماية، أو لضمان واحد أو أكثر من الجوانب التالية:

- سلامة وأمن المفوضية، وموظفيها، أو موظفي الشركاء المنفذين.
- أو الاحتياجات والأولويات التشغيلية الملحّة للمفوضية في سعيها إلى تحقيق ولايتها.

(ب) كانت هنالك أسباب تدعو إلى الاعتقاد بأن الطلب ينطوي بصورة واضحة على إساءة، أو احتيال أو عرقلة لغرض معالجة البيانات الشخصية.

٤
معالجة البيانات من قبل المفوضية

4.1 سرّية المعلومات الشخصية

4.1.1 البيانات الشخصية مصنّفة بأنها سرّية الطابع بحكم تعريفها؛ إذ يتعيّن على المفوضية احترام سرّية البيانات الشخصية عند معالجتها في جميع الأوقات.

4.1.2 لضمان تحقيق السرّية ومراعاتها، يتعيَّن حفظ البيانات الشخصية في ملفات، وتخزينها بطريقة تكون فيها متاحة للموظفين المصرّح لهم بالوصول إليها، وتحويلها فقط من خلال استعمال سبل التواصل المحمية.

4.2 أمن المعلومات الشخصية

4.2.1 يتعيّن على المفوضية كفالة وتطبيق مستوىً مرتفع من أمن البيانات، بحيث يكون ملائماً للتصدي للمخاطر التي تفرضها طبيعة البيانات الشخصية، ومعالجتها، مع توافر الأجهزة الضرورية ومستوى جودتها، وتكلفتها وجدواها التشغيلية من الناحية العملية.

4.2.2 تهدف تدابير أمن البيانات لدى المفوضية إلى حماية البيانات الشخصية من التعرض للتلف، سواءً عن طريق الخطأ أو بشكل غير قانوني / غير شرعي، أو الفقدان، أو التغيير، أو الإفصاح غير المصرّح به، أو الوصول إليها.

4.2.3 يتعيّن على المفوضية، بعد أخذ التكنولوجية المتوافرة والتكلفة بعين الاعتبار، تنفيذ تدابير تنظيمية وفنية ملائمة لضمان استيفاء عمليةُ معالجة البيانات الشخصية متطلباتِ تطبيق هذه السياسة. وهذا يشمل تنفيذ تكنولوجيات وأدوات تعزيز حماية البيانات لتمكين مجهّزي ومعالجي البيانات من توفير مستوى من الحماية أفضل للبيانات الشخصية («تأمين الخصوصية من خلال التصميم، وبشكل تلقائي»).

4.2.4 تشمل التدابير التنظيمية ما يلي:

(أ) إجراءات عمل موحّدة.

(ب) وضع تنظيم دورة تدريبية للموظفين في مجال حماية وأمن البيانات.

(ت) إجراء تقييم أثر حماية البيانات (الفقرة 4-5 من هذه السياسة).

4.2.5 تشمل التدابير الفنية ما يلي:

(أ) المحافظة على الأمن المادي للمباني، والأجهزة والمعدات المحمولة، وملفات وسجلات الحالات الفردية.

(ب) المحافظة على أمن الحواسيب وتكنولوجية المعلومات، على سبيل المثال، التحكم في الدخول (مثل كلمات السّر، والدخول المتعدد الطبقات)، والتَّحكم بالمستخدمين، والتحكم في التخزين، والتحكم في المُدخلات، والتحكم في الإرسال والنقل (كالتشفير، مثلاً).

4.2.6 في الحالات الأمنية الآخذة في التدهور، والتي تفرض خطر حدوث اختراقات خطيرة للبيانات الشخصية، يجب على المفوضية اتخاذ جميع الخطوات الضرورية والممكنة لتجنُّب اختراقات البيانات الشخصية، من خلال تغيير أماكن ملفات الحالات الفردية أو إتلافها، كحل أخير، سواءٌ أكانت ورقية أم محوسبة؛ وذلك لمنع إلحاق الأذى بأصحاب البيانات.

4.3 ضمان دقَّة البيانات الشخصية

4.3.1 يجوز للمفوضية تصحيح أو حذف البيانات الشخصية المحتفظ بها في نُظُمها، إذا كانت تلك البيانات غير دقيقة، أو غير مكتملة، أو غير ضرورية، أو زائدة عن الحاجة.

4.3.2 يجب على المفوضية تحديث سجلات البيانات الشخصية عند الضرورة، والتحقق منها بصورة دورية.

4.3.3 عندما تُصحَّح البيانات الشخصية في نُظُم المفوضية أو تُحذف منها، يتعيَّن على المفوضية إبلاغ جميع الشركاء المنفّذين و / أو الأطراف الثالثة - الذين حُوّلت إليهم البيانات الشخصية ذات الصلة، بما قامت به المفوضية من تصحيح أو حذف، وذلك في أقرب فرصة معقولة من الناحية العملية.

4.4 التبليغ عن اختراق البيانات الشخصية

4.4.1 يُطلَب من موظفي المفوضية تبليغ مراقب البيانات، في أقرب فرصة ممكنة، حالما يُصبحون على دراية بأي اختراق للبيانات الشخصية، وتسجيل ذلك الاختراق بشكل صحيح.

4.4.2 إذا كان من المحتمل أن يؤدي اختراق البيانات الشخصية إلى إلحاق الضرر أو الأذى بصاحب البيانات، فيجب على مراقب البيانات بذل قصارى جهده لإبلاغ صاحب البيانات بحدوث الاختراق في بياناته الشخصية، ولاتّخاذ تدابير تخفيفية لأثر ذلك الاختراق، حسبما تقتضي الحاجة، من دون تأخير غير مبرّر. وفي مثل هذه الحالات، يجب على مراقب البيانات إخطار مسؤول حماية البيانات عن حدوث اختراق في بياناته الشخصية.

4.4.3 يجب أن يصف التبليغ ما يلي:

(أ) طبيعة اختراق البيانات الشخصية، بما في ذلك فئات وعدد أصحاب البيانات وسجلات البيانات المعنيين كلهم بهذا الاختراق.

(ب) العواقب السلبية المعروفة والمنظورة التي تلحق باختراق البيانات الشخصية.

(ت) التدابير التي اتُّخذت أو المُقترح اتّخاذها للتّخفيف من الآثار الضارّة التي يمكن حدوثها ومعالجتها.

4.5 عمليات تقييم آثار حماية البيانات

4.5.1 قبل أن تخوض المفوضية في تفاصيل النُّظم، أو المشاريع أو السياسات الجديدة، أو قبل الدخول في اتفاقيات تحويل البيانات مع الشركاء المنفّذين، أو الأطراف الثالثة – الأمر الذي قد يؤثّر سلباً على حماية البيانات الشخصية للأشخاص المعنيين-يتعين على المفوضية إجراء تقييم أثر حماية البيانات. فعمليات التقييم هذه تكون مطلوبةً حيثما يُحتمل أن يكون جمع البيانات الشخصية ومعالجتها عملًا كبيراً ومتكرّرًا وهيكليًّا (بمعنى حيثما يتم التشارك في المعلومات مع أحد الشركاء المنفّذين أو الأطراف الثالثة على مدى فترة محدّدة من الزمان).

4.5.2 من المحتمل أن يحتوي تقييم أثر حماية البيانات على وصف عام لما هو مُتوَقَّع من النُّظم أو المشاريع أو السياسات أو اتفاقيات التشارك في البيانات، التي تشمل معالجة البيانات الشخصية؛ وعلى تحليل للمخاطر المتعلقة بحقوق أصحاب البيانات بحكم الظروف المحيطة بهم، وطبيعة البيانات الشخصية المعالجة؛ والضمانات الوقائية؛ والتدابير الأمنية وغيرها من التدابير المعمول بها أو المقترحة لضمان الامتثال لهذه السياسة.

4.5.3 يكون مراقبو البيانات مسؤولون عن تنظيم وتنفيذ تقييمات أثر حماية البيانات الشخصية، عند الحاجة. وعادة ما يتم تنفيذ هذه التقييمات على المستوى القطري ما لم يتقرر تنفيذها على المستوى العالمي أو الإقليمي بسبب نطاق النظام أو الترتيب.

4.5.4 يجب على مراقبي البيانات إبقاء مسؤول حماية البيانات على اطلاع كامل بأي تقييم يتم تنفيذه تحت مسؤوليتهم ومشاركة نسخة من التقييم معه.

4.6 الاحتفاظ بملفات الحالات

4.6.1 البيانات الشخصية التي لا تُسجّل في ملفات حالات الأفراد لا ينبغي الاحتفاظ بها لمدة أطول مما تقتضيه الضرورة للغرض (للأغراض) الذي تم جمعها لأجل تحقيقه.

4.6.2 تعتبر جميعُ ملفات حالات الأفراد، سواءٌ أكانت مفتوحة أم مغلقة، سجلات دائمة، ويتعيّن بالتالي الاحتفاظ بها بصورة دائمة بما يتوافق مع سياسة المفوضية للوصول إلى المحفوظات.[6]

6 سياسة المفوضية للوصول إلى المحفوظات: http://www.unhcr.org/3b03896a4.html.

٥

معالجة البيانات من قبل الشركاء المنفّذين

5.1 شرط عام

في الحالات التي يكون فيها جمع البيانات ومعالجتها إحدى مسؤوليات الشركاء المنفّذين، فإن البيانات الشخصية تكون قيد الجمع والمعالجة بالنيابة عن المفوضية. ولهذه الأسباب، يُتوقَّع من الشركاء المنفّذين احترام وتطبيق المعايير نفسها أو المماثلة لها والمبادئ الأساسية لحماية البيانات الشخصية، كما تضمَّنتها هذه السياسة (ولا سيما الأقسام 2، 3، 4). وهذا ينطبق سواءٌ أكانت المفوضية تعتزم تحويل البيانات الشخصية إلى الشركاء المنفّذين، أم كان الشركاء التنفيذيون يجمعون البيانات الشخصية لكي يقوموا بتنفيذ الأنشطة المتَّفق عليها.

5.2 التَّحقُّق

بالرّغم من وجود اتفاقيات شراكة (بين المفوضية والشركاء المنفّذين المعنيين)، فلا بُدَّ للمفوضية التحقق من استيفاء عملية معالجة البيانات الشخصية من قبل الشريك المنفّذ المعني للمعايير والمبادئ الأساسية لهذه السياسة؛ وذلك كله قبل تحويل البيانات الشخصية إلى الشريك المنفّذ، أو قبل إشراكه في عمليات جمع البيانات الشخصية ومعالجتها. وقد يُشكّل هذا التحقق جزءاً من عملية تقييم أثر حماية البيانات.

5.3 اتفاقيات الشراكة

يتعيّن على المفوضية مطالبة الشركاء المنفّذين بالالتزام بهذه السياسة من خلال تقديمهم تعهُّدات كجزء من التوقيع على اتفاقيات الشراكة. ومن الضروري لتلك الاتفاقيات أن تُحدّد الغرض المحدّد (الأغراض المحدّدة) لمعالجة البيانات الشخصية والأساس المشروع لذلك.

5.4 قدرة الشريك

قد يتعيّن على المفوضية مساعدة الشركاء المنفّذين في بناء أو تعزيز قدراتهم، لكي يتسنّى لهم الالتزام بمعايير حماية البيانات، وبالمبادئ التي تحتوي عليها هذه السياسة؛ فهذه المساعدة ربما تتعلّق بوضع وتعديل السياسات، وتقديم التدريب، ووضع تدابير فنية وتنظيمية موضع التنفيذ.

5.5 إنهاء الشراكة

بعد إنهاء الشراكة، سوف تُعاد جميع البيانات الشخصية التي جُمعت في إطار تنفيذ الشراكة إلى المفوضية. وقد تنصُّ اتفاقيات الشراكة على وجود استثناءات من إعادتها، ولا سيما في الحالات التي تتوافر فيها أسباب مشروعة لوضع الاستثناءات، وعلى وجه التحديد، الحصول على موافقة أصحاب البيانات أنفسهم.

٦
تحويل البيانات الشخصية إلى الأطراف الثالثة

6.1 الشَّروط العامة

6.1.1 يجوز للمفوضية تحويل البيانات الشخصية إلى الأطراف الثالثة على شرط أن تكون تلك الأطراف قادرة على توفير مستوى من حماية البيانات مماثل للمستوى الذي توفّره هذه السياسة، أو شبيه بها.

6.1.2 بالنظر إلى المخاطر المحتملة لحماية البيانات، والتي تنطوي عليها عمليات تحويل البيانات إلى أطراف ثالثة، يتعيّن على المفوضية إيلاء اهتمام خاص بالمبادئ الأساسية لهذه السياسة:

(أ) أن يستند تحويل البيانات الشخصية إلى سبب واحد أو أكثر من الأسباب المشروعة.

(ب) أن يكون تحويل البيانات الشخصية لغرض واحد محدد ومشروع أو أكثر من الأغراض المحددة والمشروعة.

(ت) أن تكون البيانات الشخصية التي يُعتَزَمُ تحويلها تفي بالغرض، ومهمّة وذات صلة، وضرورية وغير زائدة عن الحاجة فيما يتعلّق بالغرض (بالأغراض) الذي تُحوَّل لأجله.

(ث) أن يكون صاحب البيانات قد جرى إبلاغه - إما عندما جُمعت البيانات وفق الفقرة 3-1، أو بعد ذلك -عن تحويل بياناته الشخصية، ما لم يكن واحد أو أكثر من القيود المنصوص عليها في الفقرة 3-7 واجب التطبيق.

(ج) أن يراعي الطرف الثالث سرّية البيانات الشخصية المُحوَّلة إليه من المفوضية. وسواءٌ أكانت هناك اتفاقية موقّعة لتحويل البيانات بين المفوضية والطرف الثالث، أم لم تكن، يجب على المفوضية السّعي إلى الحصول على اتفاق خطي من الطرف الثالث مفاده الاحتفاظ بسرية تلك البيانات الشخصية في جميع الأوقات. ولكي يتمّ ضمان تلك السّرية ومراعاتها، يجب حفظ البيانات الشخصية وتخزينها بطريقة تكون فيها متاحة فقط للموظفين الذين يُؤذَن لهم بذلك، وتحويلها فقط من خلال استعمال وسائل تواصل محمية.

(ح) يحافظ الطرف الثالث على توفير مستوىً رفيعٍ من أمن البيانات بما يكفل حمايتها من مخاطر الإتلاف، أو الفقدان أو التغيير أو الإفصاح غير المصرّح عنها، أو إمكانية الوصول إليها، سواءٌ أكان ذلك بصورة عرضية أو غير قانونية / غير مشروعة.

6.1.3 بالإضافة إلى ذلك، يتعيّن على المفوضية ضمان ألَّا يؤثّر تحويل البيانات الشخصية سَلبًا على ما يلي:

(أ) سلامة وأمن موظفي المفوضية و / أو موظفي الشركاء المنفذين.

(ب) و / أو الأداء الوظيفي الفعّال لعمليات المفوضية، أو ولايتها، على سبيل المثال بسبب فقدان الثقة بين المفوضية والأشخاص المعنيين، أو فقدان التَّصوُّر الذهني لكيان المفوضية كمنظمة مستقلة، غير سياسية، تُعنى بالعمل الإنساني.

6.1.4 قبل الموافقة على تحويل البيانات إلى طرف ثالث، يتعيّن على المفوضية تقييم مستوى حماية البيانات لدى ذلك الطرف. ويجب على مراقب البيانات، كجزء من هذا التقييم، القيام بما يلي من جملة أمور أُخرى: تقييم القوانين، والنُّظُم الأساسية والسياسات الداخلية الواجبة التطبيق لدى الطرف الثالث، والالتزامات التعاقدية المُحدّدة، أو التّعهّدات باحترام الأُطر المحدّدة لحماية البيانات، وتنفيذها بطريقة فعّالة، إلى جانب السُّبل الفنية والتنظيمية النافذة لأمن البيانات. وعملًا بالفقرة 5-4، ربما يحتاج مراقب البيانات إلى إجراء تقييم أثر حماية البيانات.

6.2 اتفاقيات تحويل البيانات

6.2.1 ما لم توجد أسباب مُرضية بعدم القيام بذلك، وقبل تحويل البيانات الشخصية إلى طرف ثالث، يجب على مراقب البيانات السّعي إلى إبرام اتفاقية لتحويل البيانات، أو حسب الاقتضاء، إدراج فقرات شرطية لحماية البيانات ضمن الاتفاقيات الأوسع نطاقًا، وعلى وجه الخصوص في الحالات التي من المحتمل أن تكون فيها تحويلات البيانات الشخصية كبيرة الحجم، أو متكرّرة، أو هيكلية – أي في الحالات التي يتم فيها التشارك في نفس النوع (الأنواع) من البيانات مع الطرف الثالث نفسه، ولأجل الغرض ذاته، على مدى فترة من محدّدة من الزمن.

6.2.2 يجب أن تنص اتفاقيات تحويل البيانات، من جملة أمور أُخرى، على ما يلي:

(أ) دراسة الغرض (الأغراض) من تحويل البيانات، والعناصر المحددة من البيانات التي ينبغي تحويلها، إلى جانب دراسة تدابير حماية البيانات وأمن البيانات التي ينبغي وضعها موضع التنفيذ.

(ب) الطلب من الطرف الثالث التعهد بأن تدابيرُ حماية البيانات وأمن البيانات لديه تلتزم بما تُحدّده هذه السياسة.

(ت) اشتراط التشاور، والرقابة والمساءلة ووضع آليات المراجعة، لكي يتسنّى الإشراف على عملية التحويل طوال مدة صلاحية الاتفاقية.

6.2.3 يتعيّن على مسؤول حماية البيانات ومكتب الشؤون القانونية لدى المفوضية مراجعة والموافقة جميع اتفاقيات تحويل البيانات.

6.3 التحويل إلى الجهات الوطنية والمحاكم الوطنية المسؤولة عن إنفاذ القانون

6.3.1 في الظروف الملائمة، يجوز للمفوضية تحويل البيانات الشخصية إلى إحدى الجهات الوطنية المسؤولة عن إنفاذ القانون، أو إلى إحدى المحاكم الوطنية. ويجوز إجراء هذه التحويلات بناءً على طلب إما من الجهة الوطنية المسؤولة عن إنفاذ القانون وإما من المحكمة الوطنية المعنية، أو بمبادرة ذاتية من المفوضية. وقد تهمُّ التحويلات الأشخاص الذين يكونون قيد التحقيق بشأن ارتكاب جريمة مزعومة، أو قد تكون متعلّقة بضحية (بضحايا) جريمة ما، أو بالشاهد (بالشهود) على وقوع جريمة ما.

6.3.2 بالإضافة إلى الشروط العامة لتحويل البيانات الشخصية إلى الأطراف الثالثة (الفقرة 6.1 باستثناء الفقرة الفرعية 6.2.1 (ث))، يمكن للمفوضية التعاون مع طلب من هذا القبيل، وتحويل البيانات الشخصية إلى جهة وطنية مسؤولة عن إنفاذ القانون، أو إلى محكمة وطنية، فقط إذا جرى استيفاء الشروط التالية:

(أ) أن يكون التحويل ضروريًا لأغراض اكتشاف جريمة جنائية خطيرة، أو الوقاية من ارتكابها أو التحقيق فيها، أو المحاكمة عليها، ولا سيما لأجل تجنُّب خطر فوري وجوهري يُهدّد سلامة الفرد أو الجمهور وأمنهما.

(ب) أن تكون الجهة المسؤولة عن إنفاذ القانون أو المحكمة، المطالبة بتحويل المعلومات، مختصّة فيما يتعلّق باكتشاف الجريمة محلّ البحث أو الوقاية من ارتكابها، أو التحقيق فيها أو المحاكمة عليها.

(ت) أن يعمل التحويل على مساعدة الجهة المسؤولة عن إنفاذ القانون أو المحكمة، بصورة جوهرية، في متابعة تحقيق هذه الأغراض، وأن يستحيلَ الحصول على تلك البيانات الشخصية، لولا ذلك التحويل، من المصادر الأُخرى.

(ث) ألّا يتعارض التحويل، بدرجة غير متناسبة، مع حق صاحب البيانات أو حق شخص آخر من الأشخاص المعنيين في التمتّع بالخصوصية أو في الحقوق الإنسانية الأُخرى.

(ج) أن يتم الحصول على موافقة الضحايا والشهود ذوي الصلة على تحويل بياناتهم الشخصية.

6.3.3 قبل تحويل البيانات الشخصية إلى الجهة الوطنية المسؤولة عن إنفاذ القانون، أو إلى المحكمة الوطنية المختصة، يتعيّن السعي إلى الحصول على المشورة من مسؤول حماية البيانات، بالتشاور مع وحدة الحماية والأمن الوطني ضمن شعبة الحماية الدولية، ومن مكتب الشؤون القانونية، والمكتب المعني (المكاتب المعنية).

6.4 الوكالة الدولية لإنفاذ القانون، أو المحاكم الدولية، أو هيئات التحكيم الدولية، أو الهيئات الدولية الأُخرى

يتعيّن إحالة طلبات تحويل البيانات الشخصية المقدّمة من كل من: المحكمة الجنائية الدولية، والمحاكم الجنائية الدولية الخاصة، ولجان تقصي الحقائق المُكلّفة من قِبَل الأمم المتحدة، والهيئات الدولية المماثلة لها، إلى شعبة الحماية الدولية (مسؤول حماية البيانات، وحدة الحماية والأمن الوطني، ووحدة الاتصال المعنية بحقوق الإنسان، حسب الاقتضاء)، ومكتب الشؤون القانونية.

6.5 الامتيازات والحصانات

تُحوَّل البيانات الشخصية من دون المساس بالامتيازات والحصانات الخاصة بالمفوضية التي تنص عليها اتفاقية امتيازات الأمم المتحدة وحصاناتها للعام 1946، ويجب ألا يُفسّر التحويل بأنه يخلُّ بتلك الامتيازات والحصانات. فامتيازات وحصانات المفوضية وموظفيها موجودة بصرف النظر عن أي اتفاقية تعاون مع حكومة البلد. وينبغي توجيه أي استفسارات بشأن تلك الامتيازات والحصانات إلى مكتب الشؤون القانونية لدى المفوضية.

٧
المساءلة والمراقبة

7.1 هيكل المساءلة والمراقبة

يتكوّن هيكل المساءلة والمراقبة المشار إليه في الفقرة 2-9 من الأطراف الفاعلة الأساسية التالية:

(أ) الموظف المسؤول عن حماية البيانات ضمن شعبة الحماية الدولية في المقر الرئيسي للمفوضية.

(ب) مراقبي البيانات في كل مكتب قُطري / عملية قُطرية.

(ت) ضبّاط الارتباط (مسؤولي الاتصال والتنسيق) في المكاتب القُطرية / العمليات القُطرية.

7.2 مراقب البيانات وضابط ارتباط حماية البيانات

7.2.1 مراقب البيانات مسؤول عن تأسيس عملية معالجة البيانات الشخصية والإشراف عليها في إطار مسؤولياته. وبناءً على ذلك، يتحمل مراقبو البيانات المسؤولية الرئيسية عن الالتزام بهذه السياسة. وتحقيقًا لهذه الغاية، يجب على مراقب البيانات تعيين ضابط ارتباط مختص بحماية البيانات، ومن حيث المبدأ، يجب أن يكون ضابط الارتباط المعيَّن، هو الموظف الأقدم رتبةً، والمسؤول عن الحماية لدى المفوضية، في المكتب القُطري / العملية القُطرية.

7.2.2 يتعيّن على مراقب البيانات تنفيذ هذه السياسة، من جملة أمور أُخرى، بمساعدة ضابط ارتباط حماية البيانات:

(أ) تحديد الأساس المشروع الواجب التطبيق للأغراض المشروعة والمحددة لعملية معالجة البيانات.

(ب) ضمان تنفيذ التدابير التنظيمية والأمنية، إلى جانب تقييم مستوى أمن البيانات لدى الأطراف الثالثة.

(ت) وضع إجراءات داخلية، ومنها على سبيل المثال، إجراءات العمل الموحدة الخاصة بحماية البيانات، تُغطي جميع الجوانب ذات الصلة بهذه السياسة، وعلى وجه الخصوص، ما يتعلّق منها باحترام حقوق صاحب البيانات، إضافةً إلى وضع تدابير أُخرى تستهدف ضمان المحافظة على سرّية وأمن البيانات.

(ث) ضمان إدراج جوانب حماية البيانات وأمن البيانات، على نحو يفي بالغرض، في تنفيذ الاتفاقيات المبرمة مع الشركاء المنفّذين.

(ج) التفاوض مع الأطراف الثالثة، حسب الاقتضاء وعلى النحو الواجب القيام به، بشأن اتفاقيات تحويل البيانات وإبرامها.

7.2.3 عند الضرورة، يجب على مراقب البيانات و / أو ضابط ارتباط حماية البيانات السَّعي إلى الحصول على المشورة من مسؤول حماية البيانات فيما يتعلّق بالاستفسارات المتعلقة بتطبيق هذه السياسة وتفسيرها.

7.3 مسؤول حماية البيانات

1-3-7 تقوم المفوضية بتعيين مسؤول حماية البيانات، يعمل ضمن شعبة الحماية الدولية في المقر الرئيسي للمفوضية، وتشمل مهام هذا المسؤول ما يلي:

(أ) إسداء المشورة، وتقديم الدعم والتدريب بشأن حماية البيانات وهذه السياسة.

(ب) المحافظة على وجود قوائم بالمعلومات التي يقدمها مراقبو البيانات، وضبّاط ارتباط حماية البيانات، وتشمل هذه القوائم اتفاقيات تحويل البيانات، وأمثلة محدّدة على مشاركة المفوضية البيانات مع الأطراف الثالثة، وعمليات تقييم أثر حماية البيانات، وإخطارات خرق البيانات، وشكاوى أصحاب البيانات.

(ت) تشجيع مراقبي البيانات والأطراف الفاعلة الأُخرى ذات الصلة لكي تَنْشط في وضع تدابير تهدف إلى الالتزام بهذه السياسة.

(ث) رصد الجهود التي تُبذَل للالتزام بهذه السياسة، والإبلاغ عنها.

(ج) التواصل والتنسيق مع مكتب الشؤون القانونية، حسب اللزوم، في إطار هذه السياسة.

2-3-7 يُقدّم مسؤول حماية البيانات تقرير سنوي عن حماية البيانات، من خلال مدير شعبة الحماية الدولية، إلى مساعد المفوض السامي لشؤون الحماية.

7.4 مسؤول حماية البيانات

هذه السياسة لا تؤثّر على الوظيفة المكلّف بها مكتب المفتش العامة، وعلى وجه التحديد، فيما يتعلّق بتلقّي المكتب شكاوى عن أفعال سوء سلوك مزعومة، على سبيل المثال، خرق السّرية أو الاحتيال، وبإجراء التحقيقات في تلك الأفعال.[7] وبذلك، يعمل مكتب المفتّش العام على تطبيق عملية الرصد، ويتّبع هيكل الالتزام الذي تُرسي قواعده هذه السياسة.

7.5 مكتب الأخلاقيات

دعماً لهذه السياسة، سوف يُقدم مكتب الأخلاقيات التوجيه بشأن الممارسات والمعايير الأخلاقية، وسوف يُساعد في تخفيف شدّة المخاطر ذات العلاقة بتجهيز ومعالجة البيانات الشخصية، من خلال إنفاذ كلٍّ من مدوّنة قواعد السلوك لدى المفوضية، وسياسة المفوضية بشأن حماية الأشخاص من الأفعال الانتقامية («سياسة حماية المُبلِّغين عن المخالفات»).

7 المعلومات بشأن وظيفة مكتب المفتش العام، وكيفية تقديم الشكاوى متوافرة على الرابط الإلكتروني: http://www.unhcr.org/pages/52e11b746.html.