الحركة الدولية للصليب الأحمر والهلال الأحمر

شبكة الروابط العائلية

مدونة قواعد السلوك الخاصة بحماية البيانات

الإصدار 2.0

2024

مقدمة

تولّى صياغة المدونة الحالية لقواعد السلوك (المدونة) مجموعة عمل تتألف من ممثلين عن الصليب الأحمر النمساوي (كلير سكوتشر-دورينغ) والصليب الأحمر البلجيكي (فلاندرز) (أكسيل فاند فيغيت وناديا تيرويدوي) والصليب الأحمر البريطاني (مارك بينهام وإيملي نوكس) والصليب الأحمر الألماني (يوتا هيرمانز) ومكتب الصليب الأحمر بالاتحاد الأوروبي (أوليفيي جينار) واللجنة الدولية للصليب الأحمر (رومين بيرشير وماسيمو ماريلي وكاتيا غيسين) والاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر (كريستوفر راسي). وساعد أيضاً عدّة ممثلين آخرين عن هذه المنظمات في صياغة هذه المدونة، وشاركوا في المناقشات والاجتماعات وقدموا إسهامات مهمة. وبدأت مجموعة العمل المناقشات بشأن هذا المشروع في أواخر عام 2013، وعلى مدى عامين، اجتمع الأعضاء عدّة مرات في مناطق أوروبية مختلفة: ميكلين (نيسان/أبريل 2014)، وبروكسل (تموز/يوليو 2014)، وفيينا (أيلول/سبتمبر 2014)، وصوفيا (تشرين الثاني/نوفمبر 2014)، ولندن (كانون الثاني/يناير 2015). وأجرى الأعضاء أيضاً عدّة اجتماعات هاتفية ومراسلات عن طريق البريد الإلكتروني. واعتمدت مجموعة العمل المدونة بتوافق الآراء، بعد مراعاة الآراء والتعقيبات التي قدّمتها الكثير من الجمعيات الوطنية.

وقام أعضاء المجموعة المعنية بتطبيق مدونة قواعد السلوك وبعض الممثلين الآخرين من مكتب حماية البيانات ووحدة حماية الروابط العائلية التابعين للجنة الدولية بتنقيح المدونة في عام 2024. واعتمدت المجموعة المعنية بتطبيق المدونة النسخة المنقحة من المدونة بتوافق الآراء، بعد مراعاة الآراء والتعقيبات التي قدّمها أعضاؤها.

وتعدّ المدونة ضرورية نظراً إلى (1) الكثير من الأشخاص والمجموعات داخل الحركة الدولية للصليب الأحمر والهلال الأحمر الذين يعملون في شبكة الروابط العائلية، وضرورة نقل البيانات داخل الحركة وإلى أشخاص ومجموعات آخرين خارج الحركة، (2) والبيئة التنظيمية المتغيرة في أوروبا والعالم في مجال قوانين حماية البيانات ومعاييرها. وتنص المدونة على الحد الأدنى من المبادئ والالتزامات والإجراءات التي يتعين على أعضاء الحركة الامتثال لها عند معالجة البيانات في إطار شبكة الروابط العائلية. وتعمل المدونة على الامتثال لأكثر لوائح حماية البيانات صرامة، وعلى وجه الخصوص تشريعات الاتحاد الأوروبي في هذا الصدد. ويتعيّن أيضاً على الجمعيات الوطنية، عند استخدام هذه المدونة، أن تضمن الامتثال لتشريعاتها الوطنية الخاصة، التي تسري في حالة وقوع أي تعارض مع المدونة. وتمثل المدونة وثيقة مرجعية مدمجة في مجموعة التوجيهات الرئيسة للحركة التي تحكم أنشطة إعادة الروابط العائلية. ويتعين على كل عضو من أعضاء الحركة اعتماد المدونة وإدماجها في إجراءاته القياسية الخاصة.

والمدونة أداة يستطيع جميع أعضاء الحركة استخدامها لحماية الحقوق والحريات الأساسية للأفراد المشاركين في أنشطة إعادة الروابط العائلية، ولا سيما حقهم في خصوصية بياناتهم الشخصية وحمايتها. ونأمل أن تؤدي المدونة إلى غرس الثقة لدى الأفراد والجهات التنظيمية على حد سواء فيما يتعلق بعمل الحركة، ولدى أعضاء الحركة ممن يحتاجون إلى نقل بيانات فيما بينهم لمعالجة حالات إعادة الروابط العائلية.

جدول المحتويات

التعاريف

الحركة الدولية للصليب الأحمر والهلال الأحمر

هي حركة إنسانية عالمية تتمثل مهمتها في "تجنب المعاناة الإنسانية وتخفيفها أينما وجدت، وحماية الحياة والصحة، وكفالة احترام كرامة الإنسان خاصة في أوقات النزاع المسلح وحالات الطوارئ الأخرى، والعمل على الوقاية من المرض وتعزيز الصحة والرعاية الاجتماعية، والتشجيع على الخدمة التطوعية واستعداد أعضاء الحركة الدائم للمساعدة، وأخيراً تنمية إحساس عالمي بالتضامن مع جميع من يحتاجون إلى مدّ الحركة يد الحماية والمساعدة لهم".

وتتكوّن الحركة من اللجنة الدولية للصليب الأحمر (اللجنة الدولية) والجمعيات الوطنية للصليب الأحمر والهلال الأحمر (الجمعيات الوطنية) والاتحاد الدولي لجمعيات الصليب الأحمر والهلال الأحمر (الاتحاد الدولي).

الوكالة المركزية للبحث عن المفقودين

هي هيئة دائمة داخل اللجنة الدولية منشأة حسب أحكام اتفاقيات جنيف الأربع وبروتوكوليها الإضافيين والنظام الأساسي للحركة. وتتعاون الوكالة مع باقي مكونات الحركة في تنفيذ أنشطة إعادة الروابط العائلية من أجل مساعدة الأشخاص المتضررين من النزاعات المسلحة وحالات العنف الأخرى والكوارث الطبيعية والظروف الأخرى التي تقتضي استجابة إنسانية. وتضطلع الوكالة بالدور الرائد داخل الحركة في جميع المسائل المتصلة بإعادة الروابط العائلية؛ فهي التي تتولى تنسيق العمليات والعمل بصفة مستشار تقني للجمعيات الوطنية، وذلك حسب اتفاق إشبيلية لعام 1997 والتدابير التكميلية المعتمدة عام 2005 واستراتيجية إعادة الروابط العائلية للحركة عن الفترة من 2008 إلى 2018.

الجهة المسؤولة عن مراقبة البيانات

الجهة المسؤولة عن مراقبة البيانات هي أيّ مكون من مكونات الحركة يتولّى، منفرداً أو مع مكونات أخرى،[1] تحديد أغراض معالجة البيانات الشخصية وأساليبها.

الجهة المسؤولة عن معالجة البيانات

تعني الجهة المسؤولة عن معالجة البيانات شخصاً أو سلطة عامة أو جهازاً أو جهة أخرى تتولّى معالجة بيانات شخصية بالنيابة عن جهة مسؤولة عن مراقبة البيانات وبناء على تعليماتها (مثل مقدّم خدمات تكنولوجيا المعلومات).

منسّق حماية البيانات لإعادة الروابط العائلية

يعني منسّق حماية البيانات لإعادة الروابط العائلية شخصاً أو وحدة من كل مكون من مكونات الحركة، يتولّى مسؤولية التوعية بحماية البيانات وضمان امتثال أعضاء الحركة للمدونة. وينبغي أن يمتلك منسّق حماية البيانات لإعادة الروابط العائلية خلفية قوية في مجال إعادة الروابط العائلية ويفهم مبادئ حماية البيانات والتزاماتها.

الشخص موضوع البيانات

يعني الشخص موضوع البيانات فرداً يمكن تحديد هويته – بشكل مباشر أو غير مباشر– عن طريق الرجوع إلى البيانات الشخصية.[2]

ولتحديد مدى إمكانية تحديد هوية شخص ما، من الضروري النظر في جميع الوسائل التي يُرجح أن تستخدمها الجهة المسؤولة عن مراقبة البيانات أو أي فرد لتحديد هوية شخص، إما بشكل مباشر أو غير مباشر. ولكي نتحقق من أيّ الوسائل التي يُرجح أن تُستخدم لتحديد هوية فرد، من الضروري النظر في جميع العوامل الموضوعية، مثل تكلفة تحديد الهوية والمدة الزمنية اللازمة. ومن الضروري النظر في التكنولوجيا المتاحة وقت معالجة البيانات، فضلاً عن أي تطورات تكنولوجية في المستقبل. وبالتالي، لا تشمل البيانات الشخصية المعلومات المجهولة التي لا ترتبط بفرد حُدّدت هويته بالفعل أو يمكن تحديدها، أو بالبيانات التي أصبحت مجهولة بطريقة لا يمكن معها تحديد هوية الشخص موضوع البيانات أو لم يعد الإمكان معها تحديد هويته. ونظراً إلى قدرات التكنولوجيات الجديدة، يصعب ضمان عدم استخدام المعلومات المجهولة أو المعلومات التي تخضع لعملية إخفاء الهوية لتحديد الشخص

[1] يرد في الملحق 5 شرح موجز عن المراقبة والمراقبة المشتركة بين اللجنة الدولية والجمعيات الوطنية.
[2] على سبيل المثال، الشخص الذي يقدّم طلب البحث عن فرد مفقود إلى مكون من مكونات الحركة.

موضوع البيانات. وبالتالي، لا تتناول هذه المدونة مسألة معالجة المعلومات المجهولة، سواء لأغراض إحصائية أو بحثية.

وعند استخدام الخدمات المتاحة عبر الإنترنت، يمكن ربط الأفراد بمجموعة من المُعَرِّفات على شبكة الإنترنت التي تقدمها الأجهزة أو التطبيقات أو الأدوات أو البروتوكولات الخاصة بهم، مثل عناوين بروتوكول الإنترنت أو ملفات تعريف الارتباط. وقد يتركوا بيانات تدل عليهم، وعندما تُدمج هذه البيانات مع المعرفات الفريدة والمعلومات الأخرى التي تقدمها الخوادم، يمكن استخدامها لإنشاء ملفات تعريفية للأشخاص وتحديد هويتهم. وإذا كانت المعلومات من قبيل الأرقام أو بيانات المواقع أو المعرفات على الإنترنت (مثل عناوين بروتوكول الإنترنت أو ملفات تعريف الارتباط) لا تحدّد هوية فرد أو لا تجعل هوية فرد قابلة للتحديد، فتعتبر هذه المعلومات مجهولة وينبغي ألّا تعتبر بيانات شخصية.

أفراد العائلة

يمكن تصنيف الأشخاص الآتي ذكرهم ضمن أفراد العائلة:

- الأطفال المولودون في إطار الزواج وخارجه، والأطفال بالتبني، وأطفال الزوج/الزوجة
- شركاء الحياة سواء أكانوا متزوجين أم لا
- الآباء، بمن فيهم والدا الزوج أو الزوجة والآباء بالتبني
- الإخوة والأخوات المولودون للوالدين نفسها أو والدين مختلفين أو بالتبني
- الأقارب المقربون[3]
- أي شخص آخر تقوم معه علاقة عاطفية قوية، حتى ولو لم تكن العلاقة بحكم الدم.

ومن الضروري النظر في الطريقة التي يُحدّد بها فرد من العائلة في القوانين المحلية للبلدان المعنية.

القُصَّر

كل فرد يقلّ عمره عن الثامنة عشر ما لم تنص القوانين المتعلقة بحقوق الطفل على بلوغه سن الرشد قبل ذلك.

أفراد آخرون

إلى جانب الأشخاص الذين يقدّمون طلبات البحث عن المفقودين والأشخاص المفقودين، قد تتعلق أنشطة إعادة الروابط العائلية بأفراد آخرين مثل أفراد العائلة الآخرين والشهود والجيران وقيادات المجتمع المحلي والأشخاص المفقودين الآخرين وغيرهم.

البيانات الشخصية

تعني البيانات الشخصية أي معلومات ترتبط بفرد حُدّدت هويته أو يمكن تحديدها. والفرد الذي يمكن التعرّف على هويته هو الشخص الذي يمكن تحديد هويته بطريقة مباشرة أو غير مباشرة، باستخدام عامل تعريف مثل اسم أو رقم أو مواد سمعية وبصرية أو بيانات موقع أو معرِفات على الإنترنت، أو باستخدام عامل أو عدة عوامل متعلقة بالهوية المادية أو الفسيولوجية أو الوراثية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص.

ولا تشمل البيانات الشخصية المعلومات المجهولة، أي المعلومات التي: (أ) لا ترتبط بفرد حُدّدت هويته بالفعل أو يمكن تحديدها أو (ب) اعتُبرت مجهولة بطريقة لا يمكن معها تحديد هوية الشخص أو لم يعد بالإمكان معها تحديد هويته.

المعلومات الحساسة

هي المعلومات الشخصية الحساسة للغاية التي تتعلّق بحالة معينة واجهها الشخص موضوع البيانات وقد تتسبّب في ضرر خطير للغاية (مثل التمييز أو القمع) إذا أُسيء التعامل مع هذه المعلومات أو كُشف عنها. ولذلك، تقتضي البيانات الحساسة مستوى أعلى من الاهتمام والحماية. ولتحديد مدى

[3] في العديد من السياقات الاجتماعية والثقافية، يشمل مفهوم العائلة جميع الأشخاص الذين يعيشون تحت سقف واحد أو يحافظون على علاقات وثيقة الصلة ببعضهم البعض. وبالتالي، يجب فهم مفهوم العائلة على أساس الممارسة والاعتراف المجتمعيين.

حساسية البيانات، لا بد من إجراء تقييم للمخاطر بشأن الحالة التي تُنفّذ فيها أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بإعادة الروابط العائلية.

وتكون بيانات الاستدلال البيولوجي والبيانات الوراثية، وكذلك البيانات التي تتعلّق بصحة الشخص موضوع البيانات، بيانات حساسة دائماً، بغض النظر عن الحالة. وتُحدّد حساسية البيانات الأخرى على أساس كل حالة على حدة، اعتماداً على الحالة. وكقاعدة عامة وغير ملزمة، قد تتصف بالحساسية البيانات التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية/الفلسفية أو تفاصيل عن الحياة الجنسية للشخص موضوع البيانات أو توجّهه الجنسي.

وبالنسبة إلى الجمعيات الوطنية، قد يختلف نطاق البيانات الحساسة حسب التشريعات المحلية.

اختراق البيانات الشخصية

اختراق البيانات الشخصية هو اختراق أمني عرضي أو غير قانوني قد يهدّد أو يؤدي إلى تدمير بيانات شخصية عندما تُرسل أو تُخزّن أو تُعالج بطريقة أخرى، أو إلى ضياعها أو سرقتها أو تعديلها أو الكشف عنها أو الاطلاع عليها لمن لا يُصرح لهم بذلك.

يعالج/ معالجة/ مُعالج

يعالج/معالجة/مُعالج يعني أي عملية أو مجموعة عمليات تُجرى على بيانات شخصية أو مجموعة من البيانات الشخصية سواء بطرق آلية أو غيرها، مثل الجمع أو التسجيل أو التنظيم أو الترتيب أو التخزين أو التعديل أو التغيير أو الاسترجاع أو الاستشارة أو الاستخدام أو الكشف عن طريق البث أو التوزيع أو استخدام طرق أخرى للإتاحة أو الحذف. ويشكل نقل بيانات، داخل الحركة أو خارجها، عملية معالجة.

الجهة المتلقية للبيانات

تعني الجهة المتلقية للبيانات شخصاً أو سلطة عامة أو جهازاً أو جهة أخرى غير الشخص موضوع البيانات أو الجهة المسؤولة عن مراقبة البيانات أو الجهة المسؤولة عن معالجة البيانات، والتي تحصل على البيانات الشخصية.

الإحالة

الإحالة هي عملية ربط شخص ما بخدمة يحتاجها. وقد تتضمن مشاركة البيانات الشخصية للشخص المفقود، وكذلك بيانات الشخص الذي قدّم طلب البحث عن الشخص المفقود.

أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بإعادة الروابط العائلية

إعادة الروابط العائلية هو مصطلح عام يصف مجموعة من الأنشطة الرامية إلى الحيلولة دون تشتّت شمل أفراد العائلة ومساعدة الأشخاص على إعادة الاتصال بأحبائهم والحفاظ على هذا الاتصال، والكشف عن مصير الأشخاص المفقودين.

ويمكن ربط هذه الأنشطة بخدمات دعم أخرى يمكن إحالة الأشخاص المتضررين إليها، مثل خدمات الدعم النفسي والدعم النفسي والاجتماعي والخدمات الطبية والقانونية والإدارية. وقد يُتاح أيضاً للعائلات المساعدة المادية، إضافة إلى النفاذ إلى برامج إعادة التوطين وإعادة الإدماج وخدمات الرعاية الاجتماعية (لمزيد من التفاصيل، انظروا الملحق 1).

خدمات إعادة الروابط العائلية

لدى الجمعيات الوطنية وبعثات اللجنة الدولية على مستوى العالم موظفون داخل منظماتها يتولّون مسؤولية إعداد أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بها، وتنفيذها.

شبكة الروابط العائلية

عندما يتشتّت شمل العائلات ويدخل الأفراد في عداد المفقودين بسبب النزاع المسلح أو حالات العنف الأخرى أو الكوارث الطبيعية أو الهجرة أو الأزمات الإنسانية الأخرى، يجب أن نبذل قصارى جهدنا لتحديد مصيرهم وإعادة الاتصال بينهم وبين أقاربهم وجمع شملهم إذا كان ذلك ممكناً.

وتشكل خدمات إعادة الروابط العائلية التي تقدمها الجمعيات الوطنية واللجنة الدولية شبكة عالمية واحدة يطلق عليها اسم "**شبكة الروابط العائلية**". وتعمل الوكالة المركزية للبحث عن المفقودين بصفتها مستشاراً تقنياً ومنسقاً لهذه الشبكة التي تحشد الموظفين والمتطوعين على نطاق عالمي وتضمن تنفيذ أنشطة إعادة الروابط العائلية وفقاً للمبادئ والمنهجية ذاتها في جميع أنحاء العالم.

ويمكنكم الاطلاع على مزيد من المعلومات عن شبكة الروابط العائلية على الموقع الإلكتروني لإعادة الروابط العائلية: http://familylinks.icrc.org/ar/home

الشخص المستضعف

في سياق هذه المدونة، يعني الشخص المستضعف أي فرد (أ) يتضرر بشكل خاص من الأثر العاطفي والنفسي لانفصاله عن أحبائه ومن الظروف التي اضطر إلى مواجهتها، أو (2) يصعب عليه التقدير الكامل للمخاطر و/أو الفرص التي تنطوي عليها معالجة البيانات بسبب طابعها المعقد.

1- مقدمة

1-1 الغرض من هذه المدونة

تنص المدونة الحالية على الحد الأدنى من المبادئ والالتزامات والإجراءات التي يتعين على موظفي إعادة الروابط العائلية من اللجنة الدولية والجمعيات الوطنية والاتحاد الدولي الامتثال لها عند معالجة البيانات في إطار أنشطة إعادة الروابط العائلية بغرض: (1) الامتثال لمعايير وتشريعات حماية البيانات المعمول بها، (2) والسماح بالنقل السلس للبيانات الشخصية من شخص إلى آخر لأغراض أنشطة إعادة الروابط العائلية، (3) وحماية الحقوق والحريات الأساسية للأشخاص الذين يقدّمون طلبات البحث عن المفقودين، والأشخاص المفقودين، وغيرهم من الأفراد المشاركين في أنشطة إعادة الروابط العائلية، مثل الشهود أو أفراد العائلة الآخرين، وفقاً للقانون الدولي الإنساني والقانون الدولي لحقوق الإنسان والمعايير الدولية الأخرى، ولا سيما الحق في الخصوصية والحق في حماية البيانات الشخصية.

1-2 نطاق هذه المدونة

1-2-1 إعادة الروابط العائلية

تسري المدونة الحالية على عملية معالجة البيانات الشخصية في سياق أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بإعادة الروابط العائلية (انظر الملحق 1).

2-2-1 البيانات الشخصية

تسري المدونة الحالية على عملية معالجة البيانات الشخصية للأشخاص الذين يقدمون طلبات البحث عن المفقودين والأشخاص المفقودين وغيرهم من الأفراد المشاركين في أنشطة إعادة الروابط العائلية (بمن فيهم الأشخاص المتوفون) التي تجريها الجهات المسؤولة عن مراقبة البيانات.

1-3 شبكة الروابط العائلية

تمنح اتفاقيات جنيف لعام 1949 وبروتوكولاها الإضافيان لعام 1977 والنظام الأساسي للحركة والقرارات التي اعتمدها مجلس المندوبين والقرارات المعتمدة أثناء المؤتمر الدولي للصليب الأحمر والهلال الأحمر، الجهات المسؤولة عن مراقبة البيانات ولاية للمشاركة في أنشطة إعادة الروابط العائلية.

وتنفذ الجمعيات الوطنية هذه الولاية جنباً إلى جنب مع سلطاتها العامة في المجال الإنساني، ولديها دور فريد في إعادة الروابط العائلية على مستوى العالم. وهي تعمل مع السلطات العامة على تنظيم الخدمات المختلفة الهادفة إلى مساعدة ضحايا النزاعات المسلحة والكوارث الطبيعة وحالات الطوارئ الأخرى.

1-4 مبادئ الحركة وتوجيهاتها

1-4-1 المبادئ الأساسية

تؤدي الجهات المسؤولة عن مراقبة البيانات أنشطتها حسب المبادئ الأساسية التي توجه عمل الحركة: الإنسانية وعدم التحيز والحياد والاستقلال والخدمة التطوعية والوحدة والعالمية. ويجب أن تتوافق جميع عمليات معالجة البيانات التي تنفذها الجهات المسؤولة عن مراقبة البيانات في إطار خدمات إعادة الروابط العائلية مع هذه المبادئ.

2-4-1 عدم إلحاق الضرر

تبذل الجهات المسؤولة عن مراقبة البيانات في إطار خدمات إعادة الروابط العائلية كل ما في وسعها لتجنب إلحاق الضرر بالأشخاص عند معالجة بياناتهم الشخصية.

3-4-1 السرية أو قواعد الكشف عن المعلومات

عندما يشارك الأشخاص موضوع البيانات معلومات مع الجهات المسؤولة عن مراقبة البيانات، يتعين على الجهات المسؤولة عن مراقبة البيانات أن تحترم هذه المعلومات وتضمن الحفاظ على طابعها السري. وتمتثل الجهات المسؤولة عن مراقبة البيانات لجميع الالتزامات القانونية الوطنية أو الإقليمية أو الدولية المعمول بها وتخضع في عملها للقيود المبينة في هذا القسم الحالي (1-4). ومن أجل تحديد أيّ من هذه الالتزامات ينطبق، يجب الرجوع إلى: (1) أي امتيازات أو حصانات أو تنازلات عن التزامات تتمتع بها أو تقدمها الجهات المسؤولة عن مراقبة البيانات في البلد أو المنطقة المعنية، (2) وأي حماية قانونية منصوص عليها في القانون الدولي، بما في ذلك القانون الدولي الإنساني، والولاية المحددة بموجب النظام الأساسي للحركة.

4-4-1 المبادئ التوجيهية التشغيلية القائمة

تُعالج البيانات الشخصية حسب المبادئ التوجيهية لإعادة الروابط العائلية التي قدمتها شبكة الروابط العائلية، مثل *"إعادة الروابط العائلية: دليل*

للجمعيات الوطنية للصليب الأحمر والهلال الأحمر"[4]، و*"تقييم احتياجات إعادة الروابط العائلية – كتيب للجمعيات الوطنية واللجنة الدولية للصليب الأحمر"*، و*"إعادة الروابط العائلية في حالة الكوارث – دليل ميداني*، والمعايير المهنية لأنشطة الحماية.[5]

2- المبادئ الأساسية لمعالجة البيانات والتزامات الجهات المسؤولة عن مراقبة البيانات

2-1 الغرض المحدّد

تحدّد الجهات المسؤولة عن مراقبة البيانات، عند جمع البيانات، السبب (الأسباب) المحدّد والصريح والمشروع لمعالجة البيانات.

وتُعالج البيانات أساساً لإعادة الاتصال بين الأقارب الذين تشتّت شملهم بسبب النزاعات المسلحة أو حالات العنف الأخرى أو الكوارث الطبيعية أو الهجرة أو الحالات الأخرى التي تستلزم استجابة إنسانية.

وفي بعض الحالات، قد يلزم إجراء مزيد من المعالجة لأغراض الأنشطة المتعلقة بإعادة الروابط العائلية، مثلاً لأغراض حفظ السجلات أو البحث العلمي أو التاريخي أو لأغراض إحصائية. وبالتالي، قد تختلف أسباب معالجة البيانات عن تلك المحددة مبدئياً في وقت جمع البيانات. ولكن بغض النظر عن الغرض، يتعين أن تمتثل جميع عمليات معالجة البيانات لجميع قوانين حماية البيانات ذات الصلة (انظروا الملحق 1 للحصول على مزيد من التفاصيل).[6]

2-2 معالجة قانونية وعادلة

يجب أن تُجرى جميع عمليات معالجة البيانات الشخصية التي تنفذها الجهات المسؤولة عن مراقبة البيانات بموجب أساس واحد أو أكثر من الأسس القانونية التالية:

- المصلحة العامة.
- المصلحة الحيوية للشخص موضوع البيانات أو لأفراد آخرين.
- موافقة الشخص موضوع البيانات.
- المصلحة المشروعة للجهات المسؤولة عن مراقبة البيانات.
- الامتثال لالتزام قانوني.

وعند بدء عملية معالجة البيانات، يجب على الجهة المسؤولة عن مراقبة البيانات أن تحدّد أساساً قانونياً من شأنه أن يجعل معالجة البيانات قانونية. وإذا حُدّد أساس قانوني مناسب، فلا يزال الشخص موضوع البيانات قادراً على ممارسة حقوقه.[7]

2-2-1 المصلحة العامة

يُفعّل هذا الأساس القانوني عندما تكون معالجة البيانات جزءاً من الولاية الإنسانية لعضو في شبكة الروابط العائلية، على النحو المنصوص عليه في القانون الدولي أو الوطني، أو عندما تكون هذه المعالجة نشاطاً يندرج في نطاق المصلحة العامة وفقاً للقانون المعمول به. والمصلحة العامة أمر أساسي لأنشطة إعادة الروابط العائلية. ومع ذلك، لا يُعترف بها دائماً في التشريعات المحلية، ولذلك ينبغي للجمعيات الوطنية أن تتحقّق أولًا مما إذا كان قانونها المحلي يسمح لها بالاعتماد عليها كأساس قانوني لمعالجة البيانات.

وتندرج إعادة الروابط العائلية والأنشطة المتصلة بإعادة الروابط العائلية التي تجريها الجهات المسؤولة عن مراقبة البيانات في المصلحة العامة لأنها ذات طبيعة إنسانية بحتة، على النحو المبين في القسم 1-3 أعلاه. (للاطلاع على الأمثلة، انظروا الملحق 2).

---

[4] Restoring Family Links: A Guide for National Red Cross and Red Crescent Societies | International Committee of the Red Cross

[5] ترد الوثائق التوجيهية ذات الصلة في الشبكة الخارجية لإعادة الروابط العائلية.

[6] لتحديد ما إذا كان الغرض (الأغراض) من إجراء مزيد من المعالجة متوافقاً مع الغرض (الأغراض) المبدئي أم لا، ينبغي للجهة المسؤولة عن مراقبة البيانات أن تنظر في العلاقة بين الغرض (الأغراض) المبدئي والغرض (الأغراض) من إجراء مزيد من المعالجة، والسياق الذي جُمعت فيه البيانات الشخصية، بما في ذلك التوقعات المعقولة للشخص موضوع البيانات، والآثار المحتملة على الشخص موضوع البيانات.

[7] انظروا الفصل 3 من هذه المدونة.

2-2-2 المصلحة الحيوية

عندما تكون معالجة البيانات ضرورية لحماية حياة المستفيدين أو سلامتهم أو صحتهم أو كرامتهم أو أمنهم، تعتبر معالجة البيانات الشخصية في المصلحة الحيوية لهؤلاء الأشخاص. وعلى سبيل المثال، في حال كان الشخص موضوع البيانات مستضعفاً لدرجة أن تقديم خدمات إعادة الروابط العائلية سيكون مسألة منقذة للحياة.

2-2-3 موافقة الشخص موضوع البيانات

من وجهة نظر الحماية، تعتبر الموافقة ضرورية لضمان شفافية خدمات إعادة الروابط العائلية وإشراك المستفيدين فيها بشكل مباشر. وفي سياق حماية البيانات في هذه المدونة، تعدّ الموافقة أحد الأسس القانونية المطلوبة من أجل معالجة البيانات. ويجب أن تُقدّم الموافقة بشكل لا لبس فيه باستخدام أي طريقة مناسبة تعطي الإشارة الحرة والمحددة والمدروسة إلى رغبات الشخص موضوع البيانات، سواء عن طريق بيان مكتوب أو شفهي أو أي نوع آخر من البيانات أو فعل تأكيدي واضح من جانب الشخص موضوع البيانات يؤكد موافقته على معالجة بياناته.

وتوفر الموافقة أساساً قانونياً لجميع أنشطة المعالجة التي تُنفّذ لتحقيق الغرض الأصلي أو لأغراض أخرى متوافقة معه. وإذا رغبت الجهات المسؤولة عن مراقبة البيانات في بدء عمليات معالجة أخرى لأغراض إضافية وغير متوافقة، فإنها بحاجة إلى إيجاد أساس قانوني جديد أو طلب موافقة إضافية من الشخص موضوع البيانات.

ويمكن تقديم الموافقة بقيود، ويحق للشخص موضوع البيانات سحب موافقته في أي وقت. وتُسجّل تفاصيل الموافقة المقدمة ومستوى السرية المطلوب وأي قيود منطبقة ويُحتفظ بها مع البيانات الشخصية طوال عملية المراجعة.

2-2-4 المصلحة المشروعة

تُعالج البيانات الشخصية أيضاً في الظروف التي يكون من المصلحة المشروعة للجهة المسؤولة عن مراقبة البيانات القيام بهذه المعالجة، وبشرط ألّا تطغى مصالح الشخص موضوع البيانات أو حقوقه وحرياته الأساسية على تلك المصلحة المشروعة (للاطلاع على الأمثلة، انظروا الملحق 3).

2-2-5 الامتثال لالتزام قانوني

تمتثل الجهات المسؤولة عن مراقبة البيانات أيضاً لجميع الالتزامات القانونية المعمول بها عند معالجة البيانات الشخصية، مثلاً أن تمتثل للتشريعات الوطنية والإقليمية وأوامر المحاكم، وتخضع للالتزام بالمبادئ الأساسية للحركة. وقد تختلف الالتزامات القانونية بين البلدان والحالات.

2-3 التزامات المعالجة

2-3-1 المسؤولية/ المساءلة

تضمن الجهات المسؤولة عن مراقبة البيانات أن الجهات المسؤولة عن معالجة البيانات – أيّ شخص أو جهة تطّلع على البيانات الشخصية وتتصرف حسب تعليمات الجهات المسؤولة عن مراقبة البيانات – تعالج البيانات الشخصية بطريقة تمتثل لهذه المدونة. وتضمن الجهات المسؤولة عن مراقبة البيانات أيضاً أن مسؤوليات كل جهة مشاركة في معالجة البيانات الشخصية تُخصّص بوضوح وتُحدّد في الشروط التعاقدية المناسبة أو القوانين الأخرى الملزمة قانوناً.

وفي بعض الأحيان، قد تحتاج الجهة المسؤولة عن معالجة البيانات إلى توظيف جهة أخرى مسؤولة عن معالجة البيانات (أي جهة فرعية مسؤولة عن معالجة البيانات) لتنفيذ أنشطة معالجة محدّدة نيابة عن الجهة المسؤولة عن مراقبة البيانات. وإذا كان الأمر كذلك، يجب على الجهة المسؤولة عن معالجة البيانات أولًا إبلاغ الجهة المسؤولة عن مراقبة البيانات، التي تقرّر بعد ذلك ما إذا كانت ستمنح ترخيصاً للجهة الفرعية المسؤولة عن معالجة البيانات أم لا. وتخضع الجهة الفرعية المسؤولة عن معالجة البيانات للمسؤوليات والالتزامات التعاقدية نفسها التي تخضع لها الجهة المسؤولة عن معالجة البيانات.

انظروا القسم 4 أدناه للاطلاع على مزيد من المعلومات عن نقل البيانات إلى أطراف ثالثة قد لا تعالج البيانات حسب التعليمات الصادرة عن الجهة المسؤولة عن مراقبة البيانات.

2-3-2 معالجة بيانات مناسبة وذات صلة ومُحدثة

بيانات مناسبة: البيانات الشخصية التي تُعالج من خلال خدمات إعادة الروابط العائلية التي تقدمها الجهة المسؤولة عن مراقبة البيانات ستخضع للمراجعة لضمان جعلها مناسبة وذات صلة وليست زائدة عن الحد اللازم بما لا يتناسب مع الأغراض التي جُمعت وعُولجت من أجلها. وعندما تُحفظ البيانات الشخصية في السجلات، لن تخضع للمراجعة، إذ تخدم أغراضاً علمية وتاريخية وإحصائية.

دقة البيانات: تكون البيانات الشخصية دقيقة وكاملة ومحدثة بشكل كافٍ للغرض الذي جُمعت وعُولجت من أجله.

2-3-3 حماية البيانات عن طريق التصميم وبالوضع الافتراضي

عند تصميم نُظم إدارة البيانات ووضع إجراءات لجمع البيانات الشخصية، تُتّخذ تدابير تقنية وتنظيمية مناسبة لضمان تلبيتها للمتطلبات المنصوص عليها في هذه المدونة.

2-3-4 تقييم أثر حماية البيانات

في الحالات التي يرجح فيها أن تنطوي المعالجة على مخاطر كبيرة على حقوق وحريات الأشخاص موضوع البيانات، مثل عمليات النقل والنشر والكشف عن المعلومات، تجري الجهة المسؤولة عن مراقبة البيانات تقييماً لأثر حماية البيانات قبل المعالجة. وإن أمكن، تستشير الجهة المسؤولة عن مراقبة البيانات منسّق حماية البيانات لإعادة الروابط العائلية وغيره من الجهات المعنية المشاركة في إعداد مشروع معالجة البيانات،[8] من أجل تحديد وتقييم ما يلي:

- مزايا معالجة البيانات
- مصادر هذه المخاطر وطبيعتها واحتمال حدوثها وشدتها
- الإجراءات الملائمة الواجب اتخاذها لإثبات الحد من المخاطر ومعالجة البيانات الشخصية وفقاً لهذه المدونة وأي قوانين معمول بها.

ويُحدّد مستوى الخطر، وبالتالي الحاجة إلى إجراء تقييم أثر حماية البيانات، بمجموعة من العوامل التي تشمل على سبيل المثال لا الحصر، حجم أنشطة معالجة البيانات ونطاقها وسياقها، والأساليب المستخدمة لمعالجة البيانات، من قبيل استخدام التكنولوجيات المؤتمتة، وطبيعة البيانات الشخصية المعالجة ومدى حساسيتها، وضعف الشخص موضوع البيانات.

وينبغي أن يحدّ تقييم أثر حماية البيانات من خطر إلحاق الضرر بالشخص موضوع البيانات و/أو الانتهاك المحتمل لحقوق الشخص موضوع البيانات وحرياته. وتوثق الجهة المسؤولة عن مراقبة البيانات نتيجة تقييم أثر حماية البيانات وأسباب الوصول إلى تلك النتيجة. وتضمن الجهة المسؤولة عن مراقبة البيانات أيضاً أن أي خطوات متخذة نتيجة لتقييم أثر حماية البيانات تُنفّذ تنفيذاً صحيحاً وتحقق الأثر المرجو.

وفي حالة الطوارئ، قد يتعذّر إجراء تقييم أثر حماية البيانات قبل بدء معالجة البيانات. وبالتالي، يُجرى التقييم بعد المعالجة، في أقرب وقت معقول.

2-3-5 الاحتفاظ بالبيانات

عندما تنتفي الحاجة إلى البيانات الشخصية للأغراض التي جُمعت من أجلها أو لإجراء معالجة إضافية أو لإجراء معالجة على أساس مشروع/قانوني آخر، تُحفظ البيانات الشخصية في السجلات أو تحذف حسب سياسة الاحتفاظ بالبيانات الصادرة عن الجهة المسؤولة عن مراقبة البيانات (انظروا القسم 3-3 أيضاً).

وتدمج الجهة المسؤولة عن مراقبة البيانات إدارة البيانات الشخصية في إجراءاتها الداخلية، بما في ذلك تخزين البيانات لأغراض الحفظ في السجلات.

2-3-6 أمن البيانات

بناءً على إمكانية الإتاحة، تُتّخذ دائماً تدابير أمنية تقنية ومادية وتنظيمية مناسبة في كل مرحلة من مراحل عمليات معالجة البيانات بغرض الحيلولة دون تدمير البيانات الشخصية أو ضياعها أو سرقتها أو تغييرها أو الاطلاع عليها أو الكشف عنها بشكل عرضي أو غير قانوني. ولا يطّلع على البيانات الشخصية سوى موظفو الجهة المسؤولة عن مراقبة البيانات الذين يحتاجون إلى الاطلاع عليها لتقديم خدمة أو أداء مهمة معينة، مع وضع ضمانات وفرض قيود على هذا الاطلاع (انظروا الملحق 3 للحصول على مزيد من التفاصيل).

2-3-7 اختراق البيانات الشخصية

في أي وقت تدرك فيه الجهة المسؤولة عن مراقبة البيانات حدوث اختراق للبيانات الشخصية، تخطر الشخص موضوع البيانات دون تأخير لا مبرر له إذا كان هناك احتمال تعرض حقوق الشخص موضوع البيانات وحرياته لخطر كبير بسبب هذا الاختراق.

وإذا كانت الجهة المسؤولة عن مراقبة البيانات خاضعة لمتطلبات قانونية محلية محدّدة تتعلق بانتهاكات البيانات، فيجب عليها أن تنظر فيما إذا كانت ملزمة بإخطار سلطات الدولة في حالة حدوث اختراق أم لا.

وإذا أثر اختراق البيانات الشخصية على الحالات التي جرت مشاركتها مع أعضاء آخرين في شبكة الروابط العائلية، فيجب على الوكالة المركزية للبحث

[8] ينبغي إدراج جميع الأدوار المشاركة في المشروع، على سبيل المثال، مجالات تكنولوجيا المعلومات والشؤون القانونية والحماية وحفظ السجلات وإدارة المعلومات.

عن المفقودين إبلاغ الجمعيات الوطنية المعنية واللجنة الدولية دون تأخير لا مبرر له لضمان قدرة شبكة الروابط العائلية على تنسيق الاستجابة المناسبة، بما في ذلك إخطار الأشخاص موضوع البيانات المتضررين.

ويكمن الغرض من إخطار الشخص موضوع البيانات باختراق البيانات الشخصية في تقليل المخاطر التي يواجهها الشخص موضوع البيانات. وستجري الجهة المسؤولة عن مراقبة البيانات تقييماً قبل المعالجة لتحديد مستوى المخاطر التي يواجهها الشخص موضوع البيانات، وتحديد ما إذا كان يتعيّن إخطار الشخص موضوع البيانات في حالة حدوث اختراق.

وفي حال تنطبق حالة واحدة أو أكثر من الحالات التالية، يجوز أن تقرر الجهة المسؤولة عن مراقبة البيانات أنه ليس من الضروري إبلاغ الشخص موضوع البيانات باختراق البيانات الشخصية:

- نفّذت الجهة المسؤولة عن مراقبة البيانات تدابير أمنية تنظيمية أو تكنولوجية أو مادية مناسبة، وطُبّقت تلك التدابير على البيانات المتضررة من اختراق البيانات الشخصية.
- اتّخذت الجهة المسؤولة عن مراقبة البيانات تدابير لاحقة تضمن عدم احتمال تعرض حقوق الشخص موضوع البيانات وحرياته بعد ذلك لخطر شديد على وجه التحديد.
- يمكن أن يتضمن إخطار الشخص موضوع البيانات جهداً غير متناسب لا سيما بسبب الظروف اللوجستية أو الأمنية الموجودة أو عدد الحالات المعنية. وفي هذه الحالة، يجب على الجهة المسؤولة عن مراقبة البيانات أن تحدّد ما إذا كان من الملائم إصدار بيان علني أو اتخاذ إجراء مماثل يُخطر من خلاله الأشخاص موضوع البيانات بطريقة لها الفعالية ذاتها.
- يمكن أن يتعارض إخطار الشخص موضوع البيانات مع ظروف مصلحة عامة مهمة ويقوض استمرار عمليات الجهة المسؤولة عن مراقبة البيانات.
- نظراً إلى الظروف الأمنية الموجودة، قد يكون الاتصال بالشخص موضوع البيانات مسألة تعرضه للخطر أو تسبب له قلقاً شديداً.

وإذا رأت الجهة المسؤولة عن مراقبة البيانات أنه من الضروري إخطار الشخص موضوع البيانات، فيجب عليها تحديد واستخدام أفضل قناة اتصال لضمان تلقي الشخص موضوع البيانات للمعلومات بطريقة مناسبة، نظراً إلى الوضع السائد.

3- حقوق الأشخاص موضوع البيانات

3-1 المعلومات والاطلاع عليها

المعلومات: تُلزم الجهة المسؤولة عن مراقبة البيانات بتزويد الشخص موضوع البيانات بالمعلومات بطريقة شفافة. وهذا مبدأ أساسي يُطبّق بغض النظر عن الأساس القانوني لمعالجة البيانات. وينص على أنه عند جمع البيانات الشخصية، أو في أسرع وقت ممكن بعد ذلك، تتولى الجهة المسؤولة عن مراقبة البيانات تزويد الشخص موضوع البيانات بمعلومات عن معالجة بياناته الشخصية في صورة شفهية أو مكتوبة، شريطة أن تسمح القيود اللوجستية والأمنية بذلك.

وينبغي أن يتلقى الشخص موضوع البيانات تفسيرات بلغة بسيطة، إما شفهياً أو من خلال وسائل أخرى مناسبة، مثل مذكرة معلوماتية خطية. ويجب تقديم المعلومات التالية كحد أدنى:

- هوية الجهة (الجهات) المسؤولة عن مراقبة البيانات ومعلومات الاتصال بها.
- الغرض المحدّد من معالجة بياناته الشخصية.
- حقيقة أن الجهة المسؤولة عن مراقبة البيانات قد تعالج بياناته الشخصية لأغراض أخرى غير تلك المحدّدة في البداية في وقت جمع البيانات، إذا كانت متوافقة مع غرض معين مذكور أعلاه.
- حق الشخص موضوع البيانات في الاطلاع على بياناته الشخصية وتصحيحها وحذفها، وكذلك سحب موافقته والاعتراض على المعالجة والإصرار على فرض قيود معينة.
- الإشارة إلى المدة التي يُحتفظ فيها بالسجلات (فترة الاحتفاظ بالبيانات) والمعايير المستخدمة لتحديد تلك الفترة.
- حقيقة أنه يمكن مشاركة بياناته الشخصية مع أطراف ثالثة، مثل منظمات أخرى (بما فيها المكونات الأخرى للحركة)، أو سلطات الدولة في

بلد جمع البيانات أو بلد آخر، أو قد يُكشف عنها علناً، وأن موافقته مطلوبة إذا كانت بياناته الشخصية ستُستخدم على النحو الموضح.

ويجب احترام التشريعات المحلية المعمول بها ويمكن أن تتطلب من الجمعيات الوطنية إدراج معلومات إضافية للشخص موضوع البيانات.

الاطلاع: يكون من حق الأشخاص موضوع البيانات في أي وقت أن يطلبوا تأكيداً بما إذا كانت البيانات الشخصية الخاصة بهم تخضع للمعالجة أم لا. وإذا كانت هذه البيانات الشخصية محل معالجة بالفعل، يكون من حقهم الاطلاع على بياناتهم الشخصية ومعلومات عن سبب المعالجة والجهات التي لديها إمكانية الاطلاع عليها ونوع الضمانات الموضوعة.

وتقدم، عند الطلب وعندما يكون ذلك مناسباً من الناحية التقنية، نسخة من الوثيقة (الوثائق) التي تتضمن معلوماتهم الشخصية.

وقبل إعطاء الإذن بالاطلاع، ينبغي أن تقيّم الجهة المسؤولة عن مراقبة البيانات إمكانية تلبية الطلب، فضلاً عن هوية الشخص الذي يقدّم الطلب. وينبغي أن يقيّد الاطلاع على البيانات للأسباب التالية:

- تغلب المصلحة العامة، بما يشمل، على سبيل المثال لا الحصر، السرية
- مصالح حماية البيانات وحقوق الآخرين وحرياتهم
- لا يمكن تعديل الوثائق محل الاهتمام لأسباب أمنية أو حالات طوارئ
- يفتقر الطلب بشكل واضح إلى أساس أو مبالغ فيه

وتحتفظ الجهة المسؤولة عن مراقبة البيانات بسجل بطلبات الاطلاع ونتيجة هذه الطلبات، بما في ذلك فئات البيانات الشخصية المطّلع عليها و/أو الامتناع عن الاطلاع على المعلومات.

2-3 الكشف عن المعلومات لأفراد العائلة والأوصياء

يجوز لأحد أفراد العائلة أو الوصي القانوني لطفل أو شخص آخر موضوع بيانات في حالة ضعف طلب الكشف عن بيانات شخصية لأقاربه أو أبنائه. ويفترض عادة أن يكون ذلك في مصلحة الشخص موضوع البيانات وبالتالي يُوافق عليه ما لم يكن هناك سبب كافي للاعتقاد بخلاف ذلك. ويجب استشارة الشخص موضوع البيانات، حيثما أمكن، لتحديد ما إذا كان لديه اعتراض على هذا الكشف عن المعلومات.

3-3 التصحيح والحذف

التصحيح: عندما يُقدم طلب تصحيح البيانات الشخصية، يجب أن تحدّد الجهة المسؤولة عن مراقبة البيانات أولاً الشخص الذي قدّم الطلب وتحدّد مدى إمكانية تلبية الطلب. وتستجيب الجهة المسؤولة عن مراقبة البيانات بعد ذلك للطلب، خاصة إذا كانت البيانات غير دقيقة أو غير كاملة. وينطبق ذلك على البيانات المحفوظة في السجلات كذلك. وتخطر الجهة المسؤولة عن مراقبة البيانات أي جهات متلقية للبيانات بالتصحيحات المنفذة، إلّا إذا كان التصحيح غير مهم أو كانت عملية الإخطار تتطلب جهداً غير متناسب.

الحذف: من حق الشخص موضوع البيانات أن يطلب حذف بياناته الشخصية من قواعد البيانات النشطة الخاصة بالجهة المسؤولة عن مراقبة البيانات في أي حالة من الحالات التالية:

- إذا لم تعد مطلوبة للأغراض التي جُمعت من أجلها بياناته الشخصية أو لم تكن مطلوبة لعملية معالجة أخرى.
- إذا سحب الشخص موضوع البيانات موافقته على المعالجة ولم يكن هناك أساس قانوني لمعالجة بياناته الشخصية.
- إذا اعترض الشخص موضوع البيانات على معالجة بياناته الشخصية.
- إذا كانت معالجة البيانات الشخصية للشخص موضوع البيانات لا تتوافق خلافاً لذلك مع هذه المدونة أو مع التشريعات المحلية المنطبقة على الجمعيات الوطنية.

وإذا نُشرت البيانات الشخصية، تتّخذ الجهة المسؤولة عن مراقبة البيانات خطوات معقولة، بما فيها تدابير تقنية، من أجل حذف البيانات من المجال العام، بما في ذلك أية روابط أو نُسخ لتلك البيانات.

ولكن يجوز تخزين البيانات الشخصية للشخص موضوع البيانات إذا كان ذلك ضرورياً أو له ما يبرره، كما في الحالات التالية:

- لأغراض تاريخية أو إحصائية أو علمية مثل توثيق الإجراءات الذي تتخذها إحدى الجهات المسؤولة عن مراقبة البيانات عند الاضطلاع بولايتها المحددة بموجب اتفاقيات جنيف لعام 1949 وبروتوكوليها الإضافيين و/أو النظام الأساسي للحركة.

- لأسباب المصلحة العامة.
- لأغراض إنسانية طويلة الأجل.
- لإقامة مطالبات قانونية أو ممارستها أو الدفاع عنها.
- بهدف النشر من جانب أي شخص لأي مادة صحفية أو أدبية أو فنية بغرض ممارسة الحق في حرية التعبير والمعرفة.

وإضافة إلى ذلك، يجوز تخزين البيانات الشخصية للشخص موضوع البيانات في الحالات التي يلزم فيها ذلك بحكم القانون. وتوثّق الجهة المسؤولة عن مراقبة البيانات جميع الطلبات ويُخطر الشخص موضوع البيانات بأي قرارات متخذة بشأن طلبه.

وعندما تتلقى الجهات المسؤولة عن مراقبة البيانات طلباً بحذف البيانات الشخصية، تشرح تأثير حذف البيانات على توفير خدمات إعادة الروابط العائلية للشخص موضوع البيانات. وتحتفظ الجهة المسؤولة عن مراقبة البيانات بالحق في رفض طلب التصحيح أو الحذف المقدّم من الشخص موضوع البيانات إذا رأت أن الشخص ربما قدم الطلب تحت ضغط و/أو كان الحذف يعود بالضرر على مصالحه الحيوية.

وتتولّى الجهة المسؤولة عن مراقبة البيانات إخطار أي جهات متلقية للبيانات بحذف بيانات شخصية وتطلب من هذه الجهات المتلقية للبيانات حذف أي روابط أو نُسخ من تلك البيانات، إلّا إذا كانت البيانات المحذوفة غير مهمة أو إذا كان الإخطار يتطلب جهداً غير متناسب. وإذا كانت الجهات المتلقية للبيانات أعضاء في شبكة الروابط العائلية، فيجب عليهم إبلاغ الجهة المسؤولة عن مراقبة البيانات بالقرار المتخذ بشأن حذف البيانات دون تأخير لا مبرر له.

3-4 الاعتراض على المعالجة

يحق للشخص موضوع البيانات الاعتراض في أي وقت عن معالجة بياناته إذا كان الأساس القانوني للمعالجة يستند إلى المصلحة العامة أو إلى المصالحة المشروعة للجهة المسؤولة عن مراقبة البيانات. ولن تُعالج البيانات الشخصية المعنية إلّا إذا أثبتت الجهة المسؤولة عن مراقبة البيانات الأسباب المشروعة لإبطال الاعتراض ومواصلة عملية المعالجة.

وتخطر الجهة المسؤولة عن مراقبة البيانات أي جهات متلقية للبيانات بهذا الاعتراض.

5-3 الحق في سحب الموافقة

عندما يكون الأساس القانوني لمعالجة البيانات هو الموافقة، يحق للشخص موضوع البيانات سحب موافقته في أي وقت. وفي حالة حدوث ذلك، تتّخذ الجهة المسؤولة عن مراقبة البيانات جميع الخطوات المعقولة لإيقاف معالجة البيانات وحذفها. وإذا نُقلت البيانات إلى طرف ثالث، فيجب على الجهة المسؤولة عن مراقبة البيانات إبلاغه بأن الشخص موضوع البيانات قد سحب موافقته حتى يتمكن الطرف الثالث أيضاً من حذف البيانات وفقاً لذلك.

6-3 الإجراءات التصحيحية

يوجّه الشخص موضوع البيانات طلبه إلى الجهة المسؤولة عن مراقبة البيانات التي توافيه بعد ذلك بإجابة خلال فترة زمنية معقولة أو، في جميع الأحوال، في غضون أي إطار زمني يفرضه القانون.

ويتحقّق الموظفون الذي يتلقّون طلباً من الشخص موضوع البيانات من هوية الشخص موضوع البيانات باستخدام أي أسلوب معقول ويتّخذون أحد الإجراءات التالية:

- الموافقة على الطلب وإخطار الشخص موضوع البيانات الذي قدّم الطلب بكيفية تلبية طلبه.
- إخطار الشخص موضوع البيانات الذي قدّم الطلب بأسباب عدم إمكانية تلبية طلبه.
- إخطار الشخص موضوع البيانات بإمكانية تقديم شكوى ضد الجهة المسؤولة عن مراقبة البيانات.

4- أحكام خاصة بنقل البيانات

1-4 مبادئ عامة

1-1-4 معلومات أساسية

تتضمن إعادة الروابط العائلية والأنشطة المرتبطة بها عادة نقل البيانات الشخصية عبر الحدود من جهة مسؤولة عن مراقبة البيانات إلى أخرى.

وقد تحتاج الجهة المسؤولة عن مراقبة البيانات إلى نقل بيانات شخصية إلى جهات مثل منظمات غير حكومية أو منظمات دولية أو سلطات العامة أو أطراف ثالثة تكون خدماتها مطلوبة لأداء أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بها.

وتنفّذ عمليات النقل هذه بما يتماشى مع أنشطة شبكة الروابط العائلية على النحو المبين في القسم 1-3، وبهذه الصفة يتعيّن إخطار الشخص موضوع البيانات على النحو الواجب عند تنفيذ عملية النقل ولا بد من وجود أساس قانوني لإجراء عملية النقل، مثل أن تصب في المصلحة العامة أو تحمي المصالح الحيوية للشخص موضوع البيانات أو غيره من الأفراد، أو يعطي الشخص موضوع البيانات موافقته. ويجب أن تمتثل عمليات النقل أيضاً للمبادئ والتوجيهات الخاصة بالحركة المبينة في القسم 1-4.

2-1-4 المبادئ العامة المنطبقة على نقل البيانات

يشكل نقل البيانات، سواء داخل الحركة أو خارجها، عملية معالجة. وتخضع عمليات النقل بذلك للمبادئ الأساسية المبينة في الفصل الثاني والحقوق الأشخاص موضوع البيانات المبينة في الفصل الثالث. ولكن تشكل عمليات نقل البيانات عملية معالجة حساسة للغاية. وبالتالي، فإن بعض متطلبات المعالجة لها أهمية خاصة مثل عمليات تقييم أثر حماية البيانات وتقديم المعلومات إلى الشخص موضوع البيانات وأمن البيانات.

وكما هو مبين في القسم 1-3، ينبغي إخطار الشخص موضوع البيانات بعملية النقل المتوقعة بشكل مناسب لبياناته الشخصية إلى أطراف ثالثة قبل/في وقت جمع البيانات.

ومن أجل نقل البيانات الشخصية إلى أفراد أو منظمات، تُتخذ ضمانات مناسبة ومتناسبة، بما فيها تلك المبيّنة في القسمين 4-1-4 و4-1-6، ويجب وضع التدابير الأمنية التقنية والتنظيمية، بما فيها تلك المدرجة في الملحق 3. وينبغي أن تُوضع في الاعتبار حساسية البيانات ومدى الحاجة الملحة للحالة التي تتطلب العمل الإنساني والقيود اللوجستية والأمنية المبينة بالتفصيل في هذه المدونة. وفي أية حالة، يجب على الدوام أخذ مبدأ عدم إلحاق الضرر بعين الاعتبار.

3-1-4 تقييم أثر حماية البيانات في عمليات نقل البيانات

إن اشتراط إجراء تقييم أثر حماية البيانات له أهمية خاصة في سياق عمليات نقل البيانات. ولذلك، عندما يكون من المحتمل أن ينطوي نقل البيانات على مخاطر معينة على حقوق الأشخاص موضوع البيانات وحرياتهم، تجري الجهة المسؤولة عن مراقبة البيانات تقييماً لأثر حماية البيانات (انظروا الملحق 6 للاطلاع على التوجيهات) قبل عملية النقل، على النحو المبين في القسم 2-3-4 أعلاه. ويراعي تقييم أثر حماية البيانات العناصر التالية:

- القوانين واللوائح الوطنية لحماية البيانات المنطبقة على نقل البيانات.
- الظروف الأمنية واحترام حقوق الإنسان والقانون الدولي الإنساني وسلامة الأشخاص موضوع البيانات في بلد معين.
- ما إذا كانت البيانات المجهولة/الإجمالية كافية، أو إذا كان من الضروري نقل البيانات التي قد تمكّن الجهة المسؤولة عن مراقبة البيانات من تحديد الشخص موضوع البيانات.
- وسائل نقل البيانات وشروطه.
- إمكانية إنفاذ شرط تعاقدي لمنع أطراف ثالثة من نقل البيانات إلى أطراف ثالثة أخرى بعد ذلك (عمليات نقل لاحقة).
- مستوى ضعف الشخص موضوع البيانات فيما يخص احتمالية وجوب وضع ضمانات إضافية لحماية السرية وإخفاء الهوية.

وفي أي حال، ينبغي ألّا تنفّذ الجهة المسؤولة عن مراقبة البيانات عملية نقل البيانات عندما يحتمل أن تعرّض الشخص موضوع البيانات للخطر بأي شكل من الأشكال.

4-1-4 الشروط

تخضع عمليات نقل البينات للشروط الإجمالية التالية:

- يُجرى تقييم أثر حماية البيانات مسبقاً إذا كان من المحتمل أن ينطوي النقل على مخاطر كبيرة للشخص موضوع البيانات.
- يجب أن تعالج الجهة المتلقية البيانات المنقولة وفقاً للأسباب المحددة لمعالجة البيانات وأي أغراض متوافقة معها.
- تتلقى الجهة المتلقية للبيانات فقط كمية ونوع البيانات الشخصية اللازمة لتحقيق الأغراض المحدّدة أو أغراض المعالجة الأخرى.
- يجب أن يكون النقل متوافقاً مع التوقعات المعقولة للشخص موضوع البيانات.

وتقيم الجهة المسؤولة عن مراقبة البيانات المخاطر التي ينطوي عليها نقل بيانات شخصية معينة إلى مؤسسات معينة لضمان الالتزام بمبدأ عدم إلحاق الضرر.

4-1-5 توثيق عمليات نقل البيانات

ترصد الجهة المسؤولة عن مراقبة البيانات عمليات النقل، وأساليب النقل، والجهات المتلقية للبيانات الشخصية.

4-1-6 اتفاقات مشاركة البيانات

كما هو مبين في القسم 4-1-2، يجوز نقل البيانات الشخصية في حال اقتنعت الجهة المسؤولة عن مراقبة البيانات بوجود ضمانات ملائمة تكفل بها الجهة المتلقية حماية البيانات الشخصية. ويمكن تحديد الضمانات الملائمة من خلال إبرام اتفاقات بشأن مشاركة البيانات الشخصية بين الجهات المسؤولة عن مراقبة البيانات والأطراف الثالثة في الحالات التي يُتوقع فيها نقل البيانات بصفة منتظمة. وتنص هذه الاتفاقات بوضوح تام على نقل البيانات الشخصية فقط للأغراض الموضحة في الاتفاقات، وأي أغراض إضافية تتوافق معها. وتنص الاتفاقات أيضاً على التدابير الأمنية والتنظيمية التي ستنفّذ من أجل كفالة حماية البيانات خلال المعالجة.

ولا تتطلب عمليات نقل البيانات داخل الحركة إبرام اتفاقات مشاركة البيانات لأن مكونات الحركة تلتزم بأحكام هذه المدونة.

ولا بد من إشراك منسّق حماية البيانات لإعادة الروابط العائلية من أجل دعم صياغة هذه الاتفاقات أو إجراءات قانونية مماثلة.

وحتى عندما توقّع الأطراف المشاركة على الاتفاقات، قد يتغير السياق العملياتي وقد يكون من غير الآمن بعد ذلك نقل فئات معينة من البيانات إلى جهات متلقية معينة. ويتطلب ذلك إجراء تقييم مسبق بناء على مبدأ عدم إلحاق الضرر.

4-2 طرق النقل

في حالة نقل البيانات، تُستخدم تدابير ملائمة لتأمين نقل البيانات الشخصية إلى أطراف ثالثة. ويتناسب مستوى الأمن المعتمد وطريقة النقل مع طبيعة البيانات الشخصية وحساسيتها، ومع المخاطر التي يحددها تقييم أثر حماية البيانات.

5- أحكام خاصة بنشر البيانات

5-1 أحكام عامة

يشكل نشر البيانات الشخصية من جانب الجهة المسؤولة عن مراقبة البيانات عملية معالجة. وهي بهذا تخضع للمبادئ العامة المنصوص عليها في الفصل الثاني وحقوق الأشخاص موضوع البيانات المبينة في الفصل الثالث. ومع ذلك، يشكل النشر عملية معالجة حساسة للغاية. وبمجرد نشر البيانات، تفقد الجهة المسؤولة عن مراقبة البيانات والشخص موضوع البيانات، إلى حد كبير، القدرة على السيطرة على الطريقة التي تُعالج بها البيانات. ولذلك، تُتّبع كذلك المبادئ الإضافية المبينة في هذا الفصل.

وعملاً بنتائج عمليات تقييم أثر حماية البيانات وبالالتزامات القانونية المعمول بها، يجوز لخدمات إعادة الروابط العائلية التي تقدمها الجهة المسؤولة عن مراقبة البيانات نشر البيانات الشخصية لإعادة الروابط العائلية بين الأقارب الذين فرقتهم النزاعات المسلحة وحالات العنف الأخرى والكوارث الطبيعية والهجرة. وقد تتضمن هذه البيانات الأسماء والصور والحالات (مثل أن يكون الشخص على قيد الحياة أو بصحة جيدة أو جريحاً أو متوفى أو مفقوداً أو نازحاً) ويجوز نشرها على الإنترنت أو عبر وسائل الإعلام أو الملصقات أو المنشورات أو الأدوات الأخرى المناسبة.

ووفقاً للقسم 2-2-1، فإن موافقة الشخص موضوع البيانات هي الأساس المفضل لنشر البيانات الشخصية.

5-2 تقييم أثر حماية البيانات في حالة نشر البيانات

إن اشتراط إجراء تقييم لأثر حماية البيانات، المبين في القسم 2-3-4 وفي الملحق 6، له أهمية خاصة في سياق نشر البيانات.

وبالإضافة إلى العناصر المبينة في القسم 2-3-4، في سياق النشر، تُراعى العناصر التالية في تقييم أثر حماية البيانات في حالة النشر:

- القوانين واللوائح الوطنية لحماية البيانات المنطبقة على نشر البيانات.
- الظروف الأمنية واحترام حقوق الإنسان والقانون الدولي الإنساني وسلامة الأشخاص موضوع البيانات في بلد معين.
- ما إذا كانت البيانات المجهولة/الإجمالية كافية أو إذا كان من الضروري نشر البيانات التي تمكّن الجهة المسؤولة عن مراقبة البيانات من تحديد الشخص موضوع البيانات، وفي الحالة الأخيرة، ما إذا كانت هناك وسائل أخرى لحماية هوية الأشخاص موضوع البيانات ستحقق

الغرض المحدد من نشر البيانات أو تقوضه (وقد تشمل هذه الوسائل الأخرى عدم ربط صورة بأسماء أو علامات مميزة أو مواقع دقيقة أو غير ذلك).

- طريقة النشر وشروطه.
- إمكانية تنفيذ شرط يمنع الأطراف الثالثة من استخدام البيانات المنشورة.
- إمكانية تحديد المدة التي يجوز أن تظل خلالها بيانات معينة منشورة على منصة إعلام معينة وطريقة التدمير التي ينبغي استخدامها بعد انتهاء الغرض المحدد للنشر.
- قياس فائدة وملاءمة عمليات النشر من خلال إجراء الجهة المسؤولة عن مراقبة البيانات تقييمات منتظمة.
- أهمية حماية الأشخاص المستضعفين من فضول الجماهير في سياق التواصل الإعلامي العام.

وإذا كان الشخص موضوع البيانات فرداً مستضعفاً، يجب أن توضع في الحسبان، عند الاقتضاء، اعتبارات إضافية، تتضمن فرض ضمانات إضافية لحماية السرية وعدم الكشف عن هوية صاحب البيانات. والالتزام بمبدأ "عدم إلحاق الضرر" هو الطريقة الأنسب لحماية الأشخاص موضوع البيانات.

5-3 البيانات التي يجوز نشرها لإعادة الروابط العائلية

إذا جاز نشر البيانات، فيجب أن تتّبع المبادئ التوجيهية في كل سياق معين، ويمكن إتاحة المزيد من التوجيهات المحددة بشأن الفئات المحددة للأشخاص موضوع البيانات. وبناء على نتائج تقييم أثر حماية البيانات، قد تتضمن تدابير تخفيف حدة المخاطر ما يلي:

- اعتماد نهج عدم إلحاق الضرر
- اقتصار النشر على البيانات ذات الضرورة القصوى التي تتيح للقارئ/المستمع تحديد هوية الأشخاص الذين تُنشر أسماؤهم/وصورهم، وإعادة التواصل بين أقاربهم.
- حظر نشر صور الأشخاص المستضعفين إلى جانب بيانات شخصية أخرى (مثل الأسماء)، وعدم نشر عنوان أي قاصر على الإطلاق.

5-4 البيانات التي يجوز نشرها للحفظ في السجلات العامة

البيانات التي حُفظت في السجلات يمكن أن تكون متاحة للجمهور حسب التشريعات المعمول بها.

5-5 البيانات التي يجوز نشرها لأغراض التواصل الإعلامي العام

يجوز نشر البيانات الشخصية لتعزيز أنشطة إعادة الروابط العائلية و/أو رفع مستوى الوعي بالحالات محل الاهتمام، بشرط أن يمتثل النشر للتشريعات المعمول بها. ومن أجل نشر البيانات لهذا الغرض المحدّد، يجب أن تحصل الجهة المسؤولة عن مراقبة البيانات أولاً على موافقة الشخص الذي قدّم طلب البحث عن المفقودين. ويرتبط التواصل الإعلامي العام أيضاً بحرية الإعلام والتعبير وبالمساءلة العامة. ولكن كما هو الحال في أي عملية نشر، يجب اتباع المبادئ المنصوص عليها في هذه المدونة وإجراء تقييم أثر حماية البيانات.

6- تطبيق مدونة قواعد السلوك

ستساعد مجموعة معنية بتطبيق مدونة قواعد السلوك في دعم تنفيذ المدونة على الصعيد العالمي عن طريق تعزيز التعلم والتنمية المستمرين.

وإضافة إلى تقيّد الجهات المسؤولة عن مراقبة البيانات بالتشريعات الوطنية، يتعيّن عليها جميعاً أن تنفّذ المدونة الحالية على النحو التالي:

- ضمان إدماج المدونة في سياسات وتوجيهات وبرامج إعادة الروابط العائلية.
- ضمان دمج المدونة كجزء لا يتجزأ من إدارة موظفي إعادة الروابط العائلية، واستخدامها كأداة تدريب لكل جهة مسؤولة عن مراقبة البيانات.
- تعيين منسّق حماية البيانات لإعادة الروابط العائلية في أي كيان يشكل جزءاً من شبكة الروابط العائلية ومشاركة بيانات الاتصال من أجل إعداد شبكة لحماية البيانات.
- المشاركة في الدراسات الاستقصائية المنتظمة ذات الصلة بتنفيذ هذه المدونة.
- التعاون مع المجموعة المعنية بتطبيق المدونة.

- إجراء تقييمات ذاتية، والمشاركة في الحوار، وإجراء استعراضات بين الأقران وأشكال أخرى من الاستعراض على أساس طوعي من أجل ضمان التحسين والتعلم المستمرين على مستوى الحركة.

وتتولى المجموعة المعنية بتطبيق المدونة مراجعة هذه المدونة وتحديثها عند الضرورة.

7- المراجع

7-1 الصكوك/ التوجيهات القانونية

الجمعية العامة للأمم المتحدة، *مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية*، 14 كانون الأول/ديسمبر 1990.

المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

Rallo Lombarte, A., *International Standard on the protection of personal data and privacy: The Madrid Resolution: International Conference of Data Protection and Privacy Commissioners, 5 November 2009,* Spanish data protection agency, Madrid, 2009.

مجلس أوروبا، اتفاقية حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، رقم 108، 28 كانون الثاني/يناير 1981، BRON.

التوجيه رقم EC/46/95 الصادر عن البرلمان الأوروبي والمجلس بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية حركة تلك البيانات، 24 تشرين الأول/أكتوبر 1995، الجريدة الرسمية للاتحاد الأوروبي 281، 23 تشرين الثاني/نوفمبر 1995، الصفحات من 31 إلى 50.

المادة 8 من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية.

المادة 16 من معاهدة نظام عمل الاتحاد الأوروبي.

المادتان 7 و8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي.

منظمة التعاون الاقتصادي والتنمية، *مبادئ توجيهية بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود*، منشور منظمة التعاون الاقتصادي والتنمية، باريس، 2002.

منظمة التعاون الاقتصادي والتنمية، *المبادئ التوجيهية بشأن حماية المستهلك في سياق التجارة الإلكترونية*، منشور منظمة التعاون الاقتصادي والتنمية، باريس، 2000.

منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ، *إطار الخصوصية لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ*، أمانة منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ، سنغافورة، 2005.

النظام الأساسي للحركة الدولية للصليب الأحمر والهلال الأحمر، بصيغته المعدلة في عام 2006.

اللجنة الدولية للصليب الأحمر، *القرار 4 الصادر عن مجلس المندوبين لعام 2007 بشأن استراتيجية إعادة الروابط العائلية للحركة الدولية للصليب الأحمر والهلال الأحمر*، اللجنة الدولية، جنيف، 2007.

المؤتمر الدولي السابع والثلاثون لمفوضي حماية البيانات والخصوصية، *القرار بشأن الخصوصية والعمل الإنساني الدولي*، أمستردام، 2015.

المؤتمر الدولي الثالث والثلاثون للصليب الأحمر والهلال الأحمر، *القرار 4 - إعادة الروابط العائلية في ظلّ احترام الخصوصية بما في ذلك ما يتعلّق بحماية البيانات الشخصية*، 33IC/19/R4، اللجنة الدولية، جنيف، 2019.

مجلس مندوبي الحركة الدولية للصليب الأحمر والهلال الأحمر، *القرار 12 المعنون حماية البيانات الإنسانية*، CD/22/R12، اللجنة الدولية، جنيف، 2022.

7-2 المفاهيم

اللجنة الدولية للصليب الأحمر، *إعادة الروابط العائلية في حالات الكوارث: دليل ميداني*، سويسرا، اللجنة الدولية، 2009، صفحة 211.

اللجنة الدولية للصليب الأحمر، *Assessing Restoring Family Links Needs: A Handbook for National Societies and the ICRC*، اللجنة الدولية، جنيف، 2010، الصفحة 103.

اللجنة الدولية للصليب الأحمر، *Guidelines on Providing Restoring Family Links Services to Persons Separated as a Result of Migration: An Internal Document for the International Red Cross and Red Crescent Movement*، اللجنة الدولية، جنيف، 2010، الصفحة 59.

اللجنة الدولية للصليب الأحمر، *استراتيجية إعادة الروابط العائلية: تتضمن مراجع قانونية*، اللجنة الدولية، جنيف، 2009، الصفحة 64.

مورغان أوليفييه، وتيدبال- بينز، وفان ألفين دانا (المحررون)، *إدارة الجثث بعد وقوع الكوارث: دليل ميداني موجه إلى المستجيب الأول*، منظمة الصحة للبلدان الأمريكية، واشنطن العاصمة، 2009، الصفحة 53.

الملاحق

الملحق 1: أنشطة إعادة الروابط العائلية والأنشطة المرتبطة بإعادة الروابط العائلية

أنشطة إعادة الروابط العائلية – يوجد أنواع مختلفة من الأنشطة بناء على الوضع والسياق:

- ترتيب تبادل الأخبار العائلية.
- البحث عن الأفراد المفقودين.
- تسجيل ورصد الأفراد (الأطفال أو البالغين) للحيلولة دون اختفائهم وإبقاء عائلاتهم مطلعة على المستجدات بشأن أماكن وجودهم.
- لم شمل العائلات وإعادة الأشخاص إلى أوطانهم.
- جمع المعلومات عن المتوفيين وإدارتها وإحالتها إلى الجهات المعنية.
- نقل الوثائق الرسمية مثل شهادات الميلاد أو وثائق إثبات الهوية أو الشهادات الأخرى الصادرة عن السلطات.
- إصدار شهادات بالاحتجاز ووثائق أخرى تقدّم معلومات عن حالات تخص أفراداً مسجلين.
- إصدار وثائق السفر عن اللجنة الدولية.
- رصد الأشخاص الذين جُمع شملهم بأقاربهم من أجل ضمان تأقلمهم بصورة جيدة.
- تعزيز النُظم ودعمها لتحديد ما حلّ بالأشخاص المفقودين.

الأنشطة المرتبطة بإعادة الروابط العائلية – توجد خدمات إنسانية أخرى مرتبطة بأنشطة إعادة الروابط العائلية وينفذها موظفو إعادة الروابط العائلية، وهي تشمل ما يلي:

- تقديم الدعم المادي، والقانوني، والنفسي، والنفسي والاجتماعي، إلى عائلات الأشخاص المفقودين وغيرهم من الأفراد المتضررين من النزاعات المسلحة وحالات العنف الأخرى والكوارث الطبيعية والهجرة والأزمات الإنسانية الأخرى.
- تقديم الدعم إلى السلطات المعنية بشأن إدارة الرفات البشرية وتحديد هويات أصحابها بواسطة الطب الشرعي.
- مساعدة عائلات الأشخاص المفقودين، والقصر غير المصحوبين بذويهم والأشخاص المستضعفين (سواء مباشرة عن طريق شبكة الروابط العائلية أو من خلال الإحالة إلى أطراف خارجية).
- تقديم خدمات إعادة التوطين أو (الإحالة إلى) خدمات دعم إعادة الاندماج إلى الفئات المستضعفة من الأشخاص.
- الحفظ في السجلات لعدد من الاحتياجات المتنوعة، مثل الذاكرة الفردية/العائلية، والذاكرة الجماعية للإنسانية، والاحتياجات الإدارية الفردية، ومساءلة الأطراف المعنية، والبحوث التاريخية والإحصائية والطبية.
- إدارة العلاقات العامة من أجل تعزيز أنشطة الروابط العائلية والأنشطة المرتبطة بها.

الملحق 2: الأسس القانونية

أ- المصلحة العامة

تُستخدم المصلحة العامة كأساس قانون:

- عند مواجهة أزمات واسعة النطاق تستلزم تدخلاً فورياً، ويمكن للشخص موضوع البيانات أن يفهم المعلومات المقدمة وأن يتصرف بشأن معلوماته التي تُشارك و/أو تُنشر.
- عندما تكون عمليات المعالجة بالغة التعقيد وتضم جهات خارجية مختلفة مسؤولة عن المعالجة وتكنولوجيات معقدة، مما يصعب على الأشخاص موضوع البيانات تقدير مخاطر ومزايا خطوات المعالجة بشكل كامل. وإذا تعذر تحديد المصالح الحيوية للشخص موضوع البيانات أو فرد آخر (بسبب غياب الحاجة الملحة) يجوز استخدام ولاية الجهة المسؤولة عن مراقبة البيانات كأساس للمعالجة، بشرط إجراء تقييم لأثر حماية البيانات يستوفي الشروط.
- عند توزيع المساعدات في الحالات التي لا يمكن فيها الحصول على موافقة جميع المستفيدين المعنيين، والتي لا يُحتمل فيها أن تتعرض حياة وسلامة الشخص موضوع البيانات أو أشخاص آخرين لمخاطر (وفي هذه الحالة تكون المصلحة الحيوية هي الأساس الأمثل للمعالجة).
- عند معالجة بيانات شخصية لشخص موضوع بيانات محتجز. وقد يحدث هذا على سبيل المثال عندما يكون فرداً محروماً من حريته بسبب نزاع مسلح أو حالة عنف أخرى، ولم تتمكّن اللجنة الدولية (أو الجمعية الوطنية) بعد من زيارة الشخص موضوع البيانات للحصول على موافقته، ويحتمل أن تؤدي ظروف الاحتجاز السائدة في الحالة محل الاهتمام إلى منع استخدام المصلحة الحيوية كأساس قانوني.
- عند معالجة البيانات الشخصية للقصر غير المصحوبين بذويهم، الذين ليس لديهم الأهلية القانونية لتقديم موافقة مستنيرة، وعندما لا تنطبق الشروط التي من شأنها أن تؤدي إلى استخدام المصلحة الحيوية كأساس قانوني.

ب- المصلحة الحيوية

تُستخدم المصلحة الحيوية كأساس قانوني:

- عند التعامل مع حالات الطوارئ التي يعجز فيها الشخص الذي يسأل عن أحد أحبائه المفقودين عن تقديم أي ملاحظات جسدياً و/أو نفسياً عن كيفية استخدام البيانات الشخصية من قبل اللجنة الدولية و/أو الجمعية الوطنية.
- عندما يكون تقديم خدمات إعادة الروابط العائلية ضرورياً لحماية حياة المستفيدين أو سلامتهم أو صحتهم أو كرامتهم.

ج- المصلحة المشروعة

تُستخدم المصلحة المشروعة كأساس قانوني عندما تكون معالجة البيانات الشخصية ضرورية من أجل ما يلي:

- ضمان أمن نُظم المعلومات والخدمات ذات الصلة التي تقدمها نُظم المعلومات هذه والسلطات العامة وفرق الاستجابة لطوارئ الحاسب الآلي وفرق الاستجابة لحوادث أمن الحاسب الآلي والجهات المزودة لشبكات وخدمات الاتصال الإلكتروني والجهات المزودة للتكنولوجيات والخدمات الأمنية، أو التي تُتاح من خلال نُظم المعلومات المذكورة. وقد يشمل ذلك منع الاطلاع غير المصرح به على شبكات الاتصالات الإلكترونية، والحيلولة دون نشر الشفرات الخبيثة ووقف الهجمات الهادفة إلى منع الوصول إلى الخدمة، وإتلاف نُظم الحاسب الآلي ونُظم الاتصالات الإلكترونية، أو قد تشمل معالجة البيانات أثناء مسح نُظم تكنولوجيا المعلومات بحثاً عن فيروسات.
- مكافحة الغش أو السرقة وتوفير إثبات عنها، مثل التحقق من هوية المستفيدين عندما يطلبون ممارسة حقوقهم.
- عدم الكشف عن هوية أصحاب البيانات واستخدام أسماء مستعارة.
- إقامة مطالبات قانونية أو ممارستها أو الدفاع عنها، سواء كانت جزءاً من إجراء قضائي أو إداري أو إجراء خارج نطاق المحاكم، وحملة تسويق مباشرة و/أو حملة علاقات عامة. وأحد الأمثلة على ذلك هو الحاجة إلى الدفاع عن مطالبات قانونية يقدّمها مستفيد.
- الرصد الداخلي لقدرات إعادة الروابط العائلية، بما في ذلك تقييم فعالية استجابات إعادة الروابط العائلية ودعم دورات استخلاص الدروس وإجراؤها.

د- الامتثال لالتزام قانوني

اعتماداً على ظروف الجهة المسؤولة عن مراقبة البيانات، قد يشمل الامتثال لالتزام قانوني ما يلي:

- الامتثال للتشريعات الوطنية أو الإقليمية، على سبيل المثال في مجالات قانون العمل، وإعداد التقارير المالية، والاحتيال، وغسل الأموال، وما إلى ذلك.
- أوامر المحكمة.

الملحق 3: أمن البيانات

يجب معالجة البيانات الشخصية بطريقة تحافظ على سرية البيانات ونزاهتها وتوافرها. ويشمل ذلك منع الاطلاع غير المصرح به على البيانات الشخصية أو استخدامها وكذلك المعدات المستخدمة لمعالجتها.

ويقوم أي أحد يعمل تحت سلطة الجهة المسؤولة عن مراقبة البيانات وله سلطة الاطلاع على البيانات الشخصية بمعالجة هذه البيانات وفق المدونة وسياسة أمن البيانات المعمول بها على النحو المبين بمزيد من التفصيل في هذا الملحق.

ومن أجل حماية البيانات ومنع انتهاك هذه المدونة، تلتزم الجهة المسؤولة عن مراقبة البيانات بتقييم المخاطر المحددة المتأصلة في عملية المراجعة وتنفيذ تدابير للحد من تلك المخاطر. وينبغي إجراء هذا التقييم بتعاون وثيق مع فريق أمن المعلومات أو تكنولوجيا المعلومات، حيثما كان ذلك مناسباً، أو مع مستشارين خارجيين، حيث أمكن. وينبغي أن تضمن هذه التدابير مستوى ملائماً من الأمن – مع مراعاة التكنولوجيا المتاحة والظروف الأمنية واللوجستية السائدة وتكاليف التنفيذ – مقارنة بالمخاطر وطبيعة البيانات الشخصية الواجب حمايتها. ويرد في ما يلي بعض هذه التدابير:

- التدريب.
- إدارة حقوق الاطلاع على قواعد البيانات التي تحتوي على بيانات شخصية.
- الأمن المادي لقواعد البيانات.
- أمن تكنولوجيا المعلومات.
- تصنيف البيانات.
- قواعد الكتمان.
- طرق تدمير البيانات الشخصية.
- أي تدابير أخرى ملائمة.

ويتمثل الهدف من هذه التدابير في ضمان الاحتفاظ بالبيانات الشخصية في حالة آمنة من الناحية التقنية والتنظيمية، وحمايتها من التعديل أو النسخ غير المصرح به أو التلاعب أو التدمير غير القانوني أو الفقدان العرضي أو الكشف عن المعلومات على نحو غير سليم أو النقل المخالف للأصول.

وتتباين تدابير أمن البيانات بناء على عدة عوامل، وهي تشمل ما يلي:

- نوع العملية.
- طبيعة البيانات الشخصية المستخدمة وحساسيتها.
- شكل البيانات المخزنة ونسقها.
- بيئة/مكان البيانات الشخصية المحددة.
- الظروف الأمنية واللوجستية السائدة.

وينبغي أن تخضع تدابير أمن البيانات للمراجعة والتحديث المنتظمين لضمان توافق مستوى حماية البيانات مع درجة الحساسية المنطبقة على البيانات الشخصية.

وتتحمل الجهة المسؤولة عن مراقبة البيانات مسؤولية ما يلي:

- تصميم نظام لإدارة أمن المعلومات. وتحقيقاً لهذا الغرض، تضع الجهة المسؤولة عن مراقبة البيانات سياسة لأمن البيانات وتحدّثها بانتظام على أن تستند إلى معايير مقبولة دولياً وإلى تقييم للمخاطر. وعلى سبيل المثال، تتضمن هذه السياسة مبادئ توجيهية للأمن المادي وسياسة أمن تكنولوجيا المعلومات، ومبادئ توجيهية لأمن البريد الإلكتروني، ومبادئ توجيهية لاستخدام معدات تكنولوجيا المعلومات، وتصنيف تداول المعلومات، وخطة طوارئ ومبادئ توجيهية لتدمير الوثائق.
- استخدام الأدوات والإجراءات الرقمية التي تتيحها الوكالة المركزية للبحث عن المفقودين من أجل تبادل البيانات الشخصية داخل الشبكة على أوسع نطاق ممكن.
- تطوير البنية التحتية للاتصالات وقواعد البيانات للحفاظ على سلامة البيانات وسريتها بما يتوافق مع سياسة أمن البيانات.
- اتخاذ جميع التدابير الملائمة، وفقاً للمدونة الحالية، لكفالة سلامة البيانات المعالجة في نظام المعلومات الخاص بالجهة المسؤولة عن مراقبة البيانات.

1- حقوق الاطلاع على قواعد البيانات

تتحمل الجهة المسؤولة عن مراقبة البيانات مسؤولية ما يلي:

- منح الإذن بالاطلاع على قواعد البيانات التي تحتوي على بيانات شخصية.
- كفالة أمن الأدوات التي تمكّن الموظفين المصرح لهم من الاطلاع على قواعد البيانات.
- الامتثال لقواعد الأمن المشار إليها في هذا الملحق.
- ضمان تمكّن الموظفين الحاصلين على إذن الاطلاع من الامتثال للمدونة الحالية. ويشمل ذلك توفير التدريب وضمان وجود بند السرية في عقود توظيف الموظفين، التي يتعيّن توقيعها قبل منح الإذن بالاطلاع على قواعد البيانات.
- ضمان منح الإذن بالاطلاع على أساس الحاجة إلى المعرفة.
- الاحتفاظ بسجل أسماء الموظفين الحاصلين على إذن الاطلاع على كل قاعدة بيانات وتحديثه عند الضرورة، على سبيل المثال عندما يتغير دور الموظف ولا يتطلب الحصول على إذن الاطلاع على قواعد البيانات.
- الاحتفاظ، إن أمكن، بسجل يرصد أسماء الموظفين الذين مُنحوا إذن الاطلاع على قاعدة بيانات طالما ظلت البيانات التي يعالجها هؤلاء الموظفون في قاعدة البيانات. وذلك ضروري لأغراض المساءلة.

ويلتزم الموظفون بمعالجة البيانات في حدود حقوق المعالجة الممنوحة لهم.

ويجوز إخضاع الموظفين الممنوحين حقوق اطلاع أوسع أو أولئك المسؤولون عن إدارة حقوق الاطلاع لالتزامات إضافية بالسرية تنص عليها العقود.

2- الأمن المادي

تتحمل الجهة المسؤولة عن مراقبة البيانات مسؤولية ما يلي:

- وضع قواعد أمنية تحدد ضوابط الأمن الإجرائية والتقنية والإدارية للحفاظ على سرية قواعد البيانات وسلامتها وإتاحتها (سواء تتعلق بأجهزة مادية أو تكنولوجيا المعلومات)[9]
- ضمان إخطار الموظفين بهذه القواعد الأمنية وتقيّدهم بها.
- التأكد من أن الموظفين غير المصرح لهم لا يستطيعون الدخول إلى مواقع التخزين.
- وضع آليات رقابة ملائمة لضمان الحفاظ على سلامة البيانات.
- ضمان تنفيذ معايير كافية للسلامة من أخطار الكهرباء والحرائق على مواقع التخزين.
- ضمان الاحتفاظ بمستويات التخزين عند الحد الأدنى الذي تفرضه الضرورة.

[9] على سبيل المثال، قفل جهاز الكمبيوتر الخاص بكم عند مغادرة محطة العمل، وعدم ترك الوثائق الحساسة في الطابعة لفترة طويلة، وعدم إتاحة كلمات السر الخاصة بكم للعموم على مكتبكم.

3- أمن تكنولوجيا المعلومات

تلتزم الجهة المسؤولة عن مراقبة البيانات بما يلي:

- وضع قواعد أمنية تحدّد ضوابط الأمن الإجرائية والتقنية والإدارية التي تحافظ على سرية نُظم المعلومات المستخدمة وسلامتها وإتاحتها.
- وضع آليات رقابة ملائمة لضمان الحفاظ على سلامة البيانات.
- وضع قواعد أمنية محدّدة لجزء من البنية التحتية لاتصالات تكنولوجيا المعلومات أو قاعدة بيانات معينة أو قسم معين، عند الضرورة.

وتُعالج جميع المراسلات عن طريق البريد الإلكتروني، الداخلية والخارجية على السواء، التي تحتوي على معلومات شخصية على أساس الحاجة إلى المعرفة. ويُنتقى متلقو رسائل البريد الإلكتروني بعناية لتجنب النشر غير الضروري للبيانات الشخصية. وينبغي ألّا تُستخدم حسابات البريد الإلكتروني الخاصة لنقل البيانات الشخصية، إلّا إذا كانت هذه هي الأداة الوحيدة المتاحة في حالة الطوارئ.

ويجب أن يتماشى الوصول عن بعد إلى الخوادم واستخدام الأجهزة الشخصية لأغراض العمل مع معايير السلامة المنصوص عليها في سياسة أمن تكنولوجيا المعلومات الخاصة بالجهة المسؤولة عن مراقبة البيانات. وما لم يكن ذلك ضرورياً لأسباب تشغيلية تفرضها الضرورة القصوى، يجب تجنب استخدام منافذ محورية واتصالات لاسلكية غير مؤمَّنة لاسترجاع البيانات الشخصية أو تبادلها أو نقلها أو إحالتها.

ويجب أن يراعي كل موظف العناية الواجبة عند تداول البيانات الشخصية أثناء الاتصال بخوادم الجهة المسؤولة عن مراقبة البيانات عن بعد. ويجب في جميع الأحوال حماية كلمات السر، ويتعين على الموظفين التأكد من تسجيل الخروج بالشكل الصحيح من نُظم الحاسب الآلي وإغلاق برامج التصفح.

وتحتاج أجهزة الحاسب الآلي المحمولة والهواتف الذكية ومعدات الوسائط المحمولة الأخرى إلى احتياطات سلامة خاصة، لا سيما عند العمل في بيئة صعبة. ويجب تخزين معدات الوسائط المحمولة في أماكن سليمة وآمنة في جميع الأحوال.

وينبغي تجنب الاحتفاظ بالبيانات الشخصية المتعلقة بالمستفيدين في التخزين المحلي للجهاز، ما لم يكن هناك خيار آخر متاح (على سبيل المثال، لا يمكن الوصول إلى منصات إدارة وتخزين الوثائق المصرح بها)[10] و/أو في حالات الطوارئ. وفي أي حال، يجب إزالة هذه المعلومات من هذه الأجهزة بمجرد استيفاء الاستخدام المقصود.

ويجب ألّا تُستخدم الأجهزة المحمولة أو القابلة للإزالة لتخزين وثائق تحتوي على بيانات شخصية مصنفة على أنها بالغة الحساسية. وإذا لم يكن هناك مفر من هذا، فيجب نقل البيانات الشخصية إلى نُظم الحاسب الآلي الملائمة وتطبيقات قواعد البيانات حالما يكون ذلك ممكناً من الناحية العملية. وفي حالة استخدام أجهزة تحتوي على ذاكرات التخزين المعتمدة على الناقل التسلسلي العام USB أو بطاقات الذاكرة لتخزين البيانات الشخصية بصفة مؤقتة، فينبغي حفظها في مكان آمن ويجب تشفير السجلات الإلكترونية. وينبغي حذف المعلومات من الأجهزة المحمولة أو الوسائط القابل للإزالة بمجرد تخزينها بصورة صحيحة وحين لم تعد هناك حاجة لاستخدامها على هذه الأجهزة.

ويجب وضع نُظم فعالة لاستعادة البيانات وإجراءات لحفظ النُسخ الاحتياطية من أجل جميع السجلات الإلكترونية، وينبغي أن يضمن مسؤول تكنولوجيا المعلومات والاتصالات المعني تنفيذ إجراءات حفظ النُسخ الاحتياطية على أساس منتظم. ويتعيّن حفظ النُسخ الاحتياطية للبيانات الحساسة بشكل أكثر تواتراً من البيانات العادية. وينبغي أن تكون السجلات الإلكترونية مؤتمتة بحيث تسمح باستعادة البيانات بسهولة في الحالات التي يصعب فيها تنفيذ إجراءات حفظ النُسخ الاحتياطية، مثلاً بسبب الانقطاع المتكرر للكهرباء أو تعطُّل النظام أو وقوع الكوارث الطبيعية.

وعندما تصبح السجلات الإلكترونية وتطبيقات قواعد البيانات غير مطلوبة، يتعيّن على الجهة المسؤولة عن مراقبة البيانات التنسيق مع مسؤول تكنولوجيا المعلومات والاتصالات المعني لضمان حذفها بصورة دائمة.

4- واجب السرية وسلوك الموظفين

يمثل واجب السرية عنصراً مهماً في أمن البيانات الشخصية. وهو يشمل:

- توقيع جميع الموظفين والمستشارين الخارجيين على اتفاقات السرية[11] في إطار عقود العمل/الاستشارات الخاصة بهم. ويقترن ذلك بالشرط الذي يقتضي أن يعالج الموظفون البيانات حسب تعليمات الجهة المسؤولة عن مراقبة البيانات فقط.
- التزام جميع الجهات الخارجية المسؤولة عن معالجة البيانات بأحكام السرية بموجب العقد. ويقترن ذلك بالشرط الذي يقتضي أن تعالج

[10] على سبيل المثال، أداة الإجابات المتعلقة بإعادة الروابط العائلية.

[11] على سبيل المثال: اتفاق عدم الكشف عن المعلومات.

الجهات المسؤولة عن معالجة البيانات هذه البيانات حسب تعليمات الجهة المسؤولة عن مراقبة البيانات فقط.

- التطبيق الدقيق من جانب جميع الموظفين والجهات الخارجية المسؤولة عن معالجة البيانات بتصنيف تداول المعلومات وفق وضعها من حيث السرية.
- ضمان التسجيل الدقيق لأي طلبات يقدمها الأشخاص موضوع البيانات بمعالجة بياناتهم الشخصية بطريقة معينة في ملفاتهم الشخصية، ولا سيما إذا أرادوا أن تظل بياناتهم سرية ولا تُشارك مع أطراف ثالثة.

ولتقليل مخاطر اختراق البيانات، يكون الموظفون المصرح لهم دون غيرهم هم المسؤولون عن جمع وإدارة البيانات من مصادر سرية والاطلاع على الوثائق وفق تصنيف تداول المعلومات المعمول به، الذي يصنف جميع المعلومات من حيث مستوى سريتها (مثل العامة، والداخلية، والسرية، والسرية للغاية).

وينبغي أن يستخدم الموظفون تصنيف تداول المعلومات من أجل تحديد مستويات سرية البيانات التي يعالجونها، وينبغي أن يرجعوا إليها أو ينقلونها ويستخدمونها بطريقة تتلاءم مع مستوى السرية ذات الصلة.

ويجوز للموظفين الذين قسموا البيانات حسب مستوى السرية تعديل هذا المستوى في أي وقت، لا سيما عن طريق تخفيض مستوى السرية إذا رأوا أن البيانات لا تتطلب مستوى كبيراً من الحماية.

5- التخطيط للطوارئ

تتحمل الجهة المسؤولة عن مراقبة البيانات مسؤولية صياغة وتنفيذ خطة لنقل السجلات في حالات الطوارئ.

6- طرق تدمير البيانات

عندما يتقرّر أن البيانات الشخصية لم تعد ضرورية، ينبغي تدمير جميع السجلات والنُسخ الاحتياطية أو جعلها مجهولة.

وتعتمد أساساً طريقة تدمير البيانات المستخدمة على ما يلي:

- طبيعة البيانات الشخصية وحساسيتها.
- نسق البيانات وطريقة الحفظ.
- حجم السجلات الإلكترونية والورقية.

ويتعيّن على الجهة المسؤولة عن مراقبة البيانات إجراء تقييم للحساسية قبل تدمير البيانات للتأكد من استخدام تقنيات تدمير ملائمة لتدمير البيانات الشخصية.

أ- تدمير السجلات الورقية

تُدمر السجلات الورقية باستخدام طرق مثل الفرم أو الحرق، ويعني ذلك أنه لا يمكن استعادتها أو استخدامها مرّة أخرى.

وقد يتقرر تحويل السجلات الورقية إلى سجلات رقمية. وفي هذه الحالة، ينبغي تدمير جميع آثار السجلات الورقية عند تحويلها إلى صيغة إلكترونية، إلّا إذا كان الاحتفاظ بالسجلات الورقية مطلوباً بموجب القانون الوطني المعمول به، أو إذا كان من الواجب الاحتفاظ بنُسخ ورقية لأغراض الحفظ في السجلات.

ب- تدمير السجلات الإلكترونية

ينبغي أن يتولّى موظفو تكنولوجيا المعلومات والاتصالات تدمير السجلات الإلكترونية لأن استخدام الخصائص العادية على نُظم الحاسب الآلي لحذف السجلات لا يضمن بالضرورة حذفها على نحو ملائم.

وعند صدور تعليمات بهذا، يتعيّن على موظفي تكنولوجيا المعلومات والاتصالات التأكد من إزالة جميع آثار البيانات الشخصية بالكامل من نُظم الحاسب الآلي والبرامج الأخرى، بما في ذلك أي نُسخ احتياطية.

ويجب تنظيف محركات الأقراص وتطبيقات قواعد البيانات ومحو البيانات من جميع الوسائط القابلة لإعادة الكتابة مثل الأقراص المدمجة وأقراص الفيديو الرقمية والشرائح المصغرة وأشرطة الفيديو وأشرطة الصوت، التي تُستخدم لتخزين البيانات الشخصية قبل إعادة استخدامها. وينبغي رصد التدابير المادية لتدمير السجلات الرقمية رصداً دقيقاً مثل إعادة التدوير أو التهشيم أو الحرق.

ج- سجلات التخلص من البيانات

تضمن الجهة المسؤولة عن مراقبة البيانات أن جميع عقود الخدمات أو مذكرات التفاهم أو الاتفاقات أو عقود النقل أو المعالجة الخطية تنص على فترة احتفاظ. وهي الفترة الزمنية التي تخزن فيها البيانات الشخصية قبل تدميرها. ويتعين على الأطراف الثالثة إعادة البيانات الشخصية إلى الجهة المسؤولة عن مراقبة البيانات والإقرار بتدمير جميع نُسخ البيانات الشخصية، بما في ذلك البيانات الشخصية المعلن عنها إلى وكلائها ومقاوليها من الباطن المعتمدين. وينبغي الاحتفاظ بسجلات التخلص من البيانات على أن توضح توقيت وطريقة التدمير بالإضافة إلى طبيعة السجلات التي دُمرت ويجب إرفاقها بتقارير المشروع أو التقييم.

ويجوز إسناد عملية تدمير كميات كبيرة من السجلات الورقية إلى شركات متخصصة. وفي هذه الحالة، ينبغي للجهة المسؤولة عن مراقبة البيانات أن تضمن توقيع الأطراف الثالثة على اتفاقات السرية والتزامها بموجب العقد بتقديم سجلات الحذف وشهادات حذف البيانات.

7- تدابير أخرى

يستلزم أمن البيانات أيضاً وضع تدابير تنظيمية ملائمة على المستوى الداخلي، تتضمن النشر المنتظم لقواعد أمن البيانات على جميع الموظفين وإبلاغهم بالالتزامات المترتبة عليهم بموجب قانون حماية البيانات، ولا سيما بشأن التزاماتهم بالسرية.

ويتعيّن على كل جهة مسؤولة عن مراقبة البيانات أن تسند دور مسؤول أمن البيانات إلى عضو واحد أو أكثر من موظفيها (فرد يعمل في الإدارة أو في مجال تكنولوجيا المعلومات على سبيل المثال).

ويلتزم مسؤول أمن البيانات أساساً بما يلي:

- ضمان امتثال الموظفين لإجراءات الأمن المنصوص عليها في هذه المدونة والقواعد الأمنية المنطبقة المنصوص عليها فيها.
- تحديد هذه الإجراءات حسب الضرورة وعند الاقتضاء.
- إجراء تدريبات إضافية على أمن البيانات للموظفين.

الملحق 4: دليل موجز بشأن تقييم أثر حماية البيانات

يتمثل الغرض من تقييم أثر حماية البيانات في تحديد وتقييم ومعالجة المخاطر المحددة المصاحبة للبيانات الشخصية الناتجة عن بعض أنشطة إعادة الروابط العائلية. ويجب أن يؤدي تقييم أثر حماية البيانات إلى تجنب هذه المخاطر أو تقليلها أو تخفيف حدتها بطريقة أخرى. ويتمثل الهدف من الدليل الحالي لتقييم أثر حماية البيانات في تمكين موظفي إعادة الروابط العائلية من إجراء تقييم أثر حماية البيانات. ويُتاح نموذج لتقييم أثر حماية البيانات لأنشطة إعادة الروابط العائلية لكيانات شبكة الروابط العائلية في صورة وثيقة مستقلة تتضمن أمثلة لأنواع المخاطر وإجراءات التخفيف المحتملة.

ويرد فيما يلي أمثلة عن الحالات التي ينبغي فيها النظر في إجراء تقييم أثر حماية البيانات.

- المنظمة التي تعملون بها في الميدان ظلت تخزن ملفاتها على أقراص مدمجة وأوراق. وأنتم الآن ترغبون في إدخال نظام قائم على الحوسبة السحابية لتخزين الملفات. فكيف ستحددون المعلومات التي من الأفضل تخزينها وفي أي مكان؟
- دمّر إعصار تسونامي عشرات القرى الساحلية. ودخل آلاف الأشخاص في عداد المفقودين. فما هي كمية المعلومات الشخصية التي ستجمعونها من عائلات الأشخاص المفقودين؟ وهل ينبغي أن تكون المعلومات كثيرة أو عند الحد الأدنى؟ وهل ينبغي أن تتضمن بيانات حساسة مثل الحمض النووي والديانة والانتماء السياسي؟
- تضع الحكومة نظاماً لتجميع كافة المعلومات الخاصة بالأشخاص المفقودين عقب إعصار تسونامي. وتطلب منكم تقديم جميع المعلومات التي بحوزتكم عن الأشخاص المفقودين. فما هو حجم المعلومات الشخصية التي ينبغي تقديمها إلى الحكومة للمساعدة على البحث عن الأشخاص المفقودين؟ وما هي الظروف التي ينبغي فيها الكشف عن المعلومات الشخصية إلى الحكومة؟
- منظمة إنسانية أخرى تطلب منكم تقديم بيانات عن الأشخاص المقيمين في مخيم للاجئين. فهل ينبغي لكم تقديم تلك البيانات؟ وتحت أي ظروف؟ وما هي عواقب ذلك؟ وهل ستتوخى المنظمة درجة العناية نفسها التي توخيتموها أنتم في معالجة المعلومات الشخصية؟
- تخطط منظمتكم لجمع السمات البيولوجية على نطاق واسع، باستخدام تكنولوجيات جديدة تسمح لكم باستخدام تحليل بصمات الأصابع والتعرف على الوجه. فما هي الضمانات التقنية التي يجب وضعها؟ وما هي الشروط التي ينبغي وضعها في العقد مع مزود الخدمة؟ وهل سيكون المستفيدون مرتاحين لتقديم هذه المعلومات؟

- هل يجوز لكم نشر صور لأطفال غير مصحوبين بذويهم يبحثون عن أقاربهم على الإنترنت؟ وهل يجوز لكم إصدار منشورات بالأطفال المفقودين؟ وإذا كان الأمر كذلك، ففي أي ظروف وبأي شروط؟
- يعرض عليكم موقع شبكة اجتماعية أن يساعدكم على إعادة الروابط العائلية بين الأقارب الذين تشتّت شملهم عقب وقوع كارثة. فكيف يمكنكم التعاون مع هذا الموقع الإلكتروني دون تعريض البيانات الشخصية والأفراد المعنيين للخطر؟
- تخطط اللجنة الدولية غداً لزيارة أحد أماكن الاحتجاز يزعم أن أحد الأشخاص المفقودين محتجز فيها. ومع الأخذ في الحسبان اعتبارات الضرورة الملحة للحالة، هل يجوز لكم نقل طلب بحث عن شخص مفقود أو إرسال رسالة من رسائل الصليب الأحمر عن طريق البريد الإلكتروني إلى اللجنة الدولية؟

وقد لا يكفي الوقت في بعض الحالات لإجراء تقييم كامل لأثر حماية البيانات أو ربما كان تعقّد عملية المعالجة أو حساسيتها أو نطاقها لا يستلزم إجراء تقييم رسمي لأثر حماية البيانات. ومع ذلك، يجب أن يضع موظفو إعادة الروابط العائلية دائماً في الحسبان إجراء تقييم للمخاطر بشأن حماية البيانات (وتسجيله إذا أمكن) عند اتخاذ قرارات بشأن نقل البيانات. وبالتالي، يجب أن يكون موظفو ومتطوعو إعادة الروابط العائلية على دراية بعملية تقييم أثر حماية البيانات والنظر في الأسئلة التالية.

وتتضمن عملية تقييم أثر حماية البيانات عادة الخطوات التالية. وينبغي أن تظهر هذه الخطوات في تقرير أثر حماية البيانات.

ألف- تحديد النطاق

1- بناء على تعقّد عملية المعالجة وحساسيتها ونطاقها، تحديد:

- مدى ضرورة تقييم أثر حماية البيانات.
- الشخص المكلف بإجراء تقييم أثر حماية البيانات.
- الشخص المكلف بمراجعة تقييم أثر حماية البيانات واعتماده.

2- في سياق نشاط إعادة الروابط العائلية محل الاهتمام، وصف كيفية جمع البيانات الشخصية واستخدامها وتخزينها ومشاركتها مع جهات أخرى. ويشمل هذا إعداد قائمة بالجهات المعنية وكتابة وصف لتدفقات البيانات. وينبغي النظر في الأسئلة التالية:

- ما هو الغرض من المعالجة.
- ما هو نوع البيانات الشخصية التي تُجمع وممن وبمعرفة من؟
- كيف تُجمع المعلومات ويُواصل معالجتها؟
- كيف تُخزن وما هو مكان تخزينها وما هي مدة تخزينها؟
- ما هي التدابير الأمنية الموجودة؟ وهل ستخضع البيانات لأي عملية استخدام أسماء مستعارة، أو تصفية أو إخفاء الهوية من أجل حماية المعلومات الحساسة و/أو هل ستُحذف البيانات التي لا حاجة ضرورية لها؟
- إذا كانت هناك استعانة بجهات خارجية مسؤولة عن معالجة البيانات، فمن له حق الاطلاع على المعلومات؟

3- تحديد الجهات المعنية التي قد توفّر المساعدة. وقد يشمل ذلك الجهات المعنية الداخلية، مثل خبراء تكنولوجيا المعلومات أو المستشارين القانونين أو الأخصائيين النفسيين أو خبراء البرامج أو غيرهم، أو الجهات المعنية الخارجية، مثل المنظمات الأخرى أو الأجهزة الحكومية أو الأخصائيين الاجتماعيين أو القيادات المجتمعية أو الأوصياء القانونيين أو غيرهم من الجهات التي يمكن أن تهمها معالجة البيانات التي حلّلها تقييم أثر حماية البيانات، أو تؤثر عليها.

باء- التقييم

4- تحديد المخاطر التي تقع على الأفراد بسبب عملية المعالجة وعدم الامتثال لهذه المدونة. وإذا حُدّدت الجهات المعنية الداخلية و/أو الخارجية، يُرجى إجراء مناقشة ومداولة معها. ولعل أحد السبل لتحديد المخاطر هي إعداد قائمة بالتهديدات ومواطن الضعف الخاصة بجميع مبادئ المدونة والمخاطر التي تنشأ عن هذه التهديدات ومواطن الضعف.

5- تقييم المخاطر من ناحية احتمالية حدوث الأثر وحدّته.

6- تحديد تدابير تجنب هذه المخاطر أو التقليل منها أو تخفيف حدتها بطريقة أخرى.

7- اقتراح توصيات، مثل التغييرات التقنية والتنظيمية أو التغييرات على استراتيجية حماية البيانات برمتها.

جيم- الموافقة والتنفيذ

8- تقديم طلب إلى خبراء حماية البيانات[12] لاستعراض التقييم والحصول على الموافقة من الموظفين المسؤولين.[13]

9- تنفيذ التوصيات المتفق عليها.

10- تحديث تقييم أثر حماية البيانات في حالة وجود تغييرات على النشاط.

وفي حالة إجراء تقييم أثر حماية البيانات، ينبغي توضيح ذلك في تقرير (يتضمن معلومات عن الأقسام "ألف" و"باء" و"جيم" المذكورة أعلاه). وبناء على تعقّد عملية المعالجة وحساسيتها ونطاقها، قد يكون تقرير تقييم أثر حماية البيانات (نتيجة عملية تقييم أثر حماية البيانات) موجزاً للغاية أو أكثر شمولاً وتفصيلاً. ويمكن لتقرير تقييم أثر حماية البيانات إدماج النموذج المتاح للجمعيات الوطنية.

الملحق 5: المراقبة والمراقبة المشتركة

يعمل عضو في شبكة الروابط العائلية، سواء كانت اللجنة الدولية أو الجمعية الوطنية، بصفة الجهة المسؤولة عن مراقب البيانات عند استيفاء الشرطين التاليين:

- الكيان الوحيد في شبكة الروابط العائلية الذي يقدم خدمات إعادة الروابط العائلية. وعلى سبيل المثال، يكون هو المنظمة الوحيدة التي تفتح ملف حالة محددة بشأن البحث عن المفقودين، أو تجمع رسائل الصليب الأحمر وتشاركها، أو تقدم مكالمات هاتفية.
- لا تشارك اللجنة الدولية والجمعيات الوطنية (على سبيل المثال، اللجنة الدولية وجمعية وطنية واحدة أو جمعيتان وطنيتان أو أكثر) أي حالات بحث عن المفقودين أو تقدم مبادرات أو شراكات أو خدمات جماعية أخرى.

ويعمل عضوان أو أكثر من أعضاء شبكة الروابط العائلية، أي اللجنة الدولية أو الجمعيات الوطنية، بصفة جهات مشتركة مسؤولة عن المراقبة عندما يعملون معاً على تحديد أغراض ووسائل عملية معالجة البيانات. ومن المعايير المهمة أن تكون المعالجة غير ممكنة دون مشاركة الطرفين. ولذلك، تُطبّق المراقبة المشتركة عندما يقدّم عضوان أو أكثر من أعضاء شبكة الروابط العائلية خدمة معينة من خدمات إعادة الروابط العائلية إلى المستفيدين الذين يحتاجون إلى جمع البيانات الشخصية واستخدامها من أجلهم. وعلى سبيل المثال، يحدث ذلك عندما يعالجون عدداً مشتركاً من حالات البحث عن المفقودين.

[12] المستشارون القانونيون والمستشارون الخارجيون المعنيون بحماية البيانات.

[13] على سبيل المثال، منسق حماية البيانات لإعادة الروابط العائلية، إن وجد. أو بدلاً من ذلك، ينبغي أن يوافق الشخص المسؤول عن أنشطة إعادة الروابط العائلية على تقييم أثر حماية البيانات.