Mis à jour et présenté à la 38e Conférence internationale des commissaires à la protection des données et de la vie privée, à Marrakech, du 17 au 20 octobre 2016.

GUIDE SUR LA COOPÉRATION DANS L'APPLICATION DES LOIS

PRÉPARÉ PAR:

Commissariat à la protection de la vie privée du Canada

et

le Commissariat à l'information du Royaume-Uni

Commissariat
à la protection de
la vie privée du Canad

ico.
Information Commissioner's Office

TABLE DES MATIÈRES

INTRODUCTION

L'Entente mondiale de coopération transfrontière dans l'application des lois (« l'Entente », présentée à l'**annexe A**) de la Conférence internationale des commissaires à la protection des données et de la vie privée (« la Conférence ») est une « déclaration d'intention générale » en vue d'assurer la coopération entre les autorités d'exécution des lois sur la protection de la vie privée[1] et propose un cadre pour y parvenir.

Les autorités qui souhaitent participer à l'Entente auront sans doute des interrogations concernant la mise en œuvre pratique de la coopération dans l'application des lois. Chaque autorité prendra elle-même ses décisions à l'interne concernant la façon dont elle participera à l'Entente (ou à la coopération dans l'application des lois en général). Toutefois, comme il peut s'agir d'un nouveau champ d'exploration pour de nombreuses autorités, il nous semble logique de nous épauler mutuellement et d'apprendre les uns des autres à cette étape préliminaire. Dans le présent guide, le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Royaume-Uni, en tant que coprésidents de l'ancien Groupe de travail sur la coopération internationale dans l'application des lois qui a élaboré l'Entente, s'efforcent de faire part de l'expérience que nous avons acquise ou que nous avons été à même d'observer grâce à l'interaction avec nos partenaires des autres pays sur le front de la coopération dans l'application des lois.

Le présent guide n'est pas de nature pédagogique ni normative. Il vise plutôt à donner une orientation utile aux autorités désireuses de coopérer dans l'application des lois. Plus précisément, il a pour objet de fournir :

i. une liste non exhaustive des enjeux que pourrait rencontrer quiconque se prépare à coopérer ou coopère dans l'application des lois;
ii. des modèles, des approches et des solutions éventuelles que les autorités pourraient envisager de mettre en œuvre pour intervenir à l'égard de ces enjeux;
iii. des facteurs à prendre en compte pour déterminer parmi les stratégies proposées lesquelles pourraient être appropriées dans certaines situations.

Les autorités devraient toujours faire preuve de souplesse dans l'application des approches présentées dans le présent guide. Chaque élément de la situation (p. ex. autorités pertinentes, législation, enjeux, parties à un dossier, etc.) nécessite une approche unique en son genre. Il pourrait aussi s'agir d'une forme hybride des approches présentées en détail dans le présent guide, voire d'une approche novatrice complètement différente que nous n'avons pas envisagée ci-après.

[1] Pour les besoins du présent guide, l'expression « autorités d'exécution des lois sur la protection de la vie privée » englobe les autorités de protection des données. De même, la notion de « protection de la vie privée » englobe la protection des données.

Avantages de la coopération dans l'application des lois

Puisque les organisations qui traitent les données personnelles sont de plus en plus présentes à l'échelle multinationale, à la fois physiquement et dans le secteur du commerce numérique (notamment en raison de l'externalisation de fonctions opérationnelles clés), la fluidité et la fréquence de la circulation transfrontière de l'information font de la coopération internationale dans l'application des lois un outil nécessaire pour promouvoir le droit à la vie privée, tant à l'échelle nationale qu'internationale. Dans le vrai sens du terme, cette coopération peut améliorer l'efficience et renforcer la capacité. C'est un élément particulièrement important dont il faut prendre acte et que l'on pourrait même faire valoir comme leçon tirée des récentes coupures exercées de façon générale par les gouvernements dans les ressources budgétaires des autorités d'exécution des lois sur la protection de la vie privée durant la crise financière mondiale. Il pourrait être bon pour l'indépendance des autorités de s'attacher à stimuler la coopération avec d'autres entités indépendantes dans un climat aussi difficile pour aider à compenser les ravages des coupures et amortir le choc des pressions politiques à l'échelle nationale. Il n'est donc pas étonnant que la coopération dans l'application des lois sur la protection de la vie privée soit en pleine progression, avec la mise en œuvre de mécanismes mondiaux novateurs comme l'Entente de la Conférence et l'outil d'alerte du GPEN. Les expériences initiales ont d'ailleurs déjà fait la preuve des avantages potentiels de la coopération :

i. Les autorités peuvent obtenir des résultats de façon plus efficiente grâce à une enquête ou à une mesure concertée d'application de la loi au lieu de prendre plusieurs mesures faisant double emploi.

ii. En travaillant ensemble, les autorités peuvent tirer parti de leur « poids » cumulatif et de leurs points forts relatifs afin que leurs mesures d'application des lois donnent des résultats plus étendus ou transversaux qu'elles ne pourraient obtenir individuellement.

iii. Grâce à l'échange de renseignements et à l'entraide dans les enquêtes, les autorités pourraient être en mesure de mener ou de faciliter des activités d'application de la loi ou des enquêtes qui comprennent des activités à l'extérieur de leur propre territoire.

iv. Au cours du processus de coopération, chaque autorité peut apprendre grâce aux connaissances et à l'expérience des autres et renforcer par le fait même son propre savoir-faire.

v. Le milieu mondial de l'application des lois sur la protection de la vie privée fait savoir aux organisations traitant des données personnelles ainsi qu'aux particuliers partout dans le monde que nous regroupons nos efforts et que nous sommes résolus à intervenir au niveau mondial pour maîtriser les risques d'atteinte à la vie privée d'envergure mondiale.

PRÉPARATION DES BASES DE LA COOPÉRATION

Établissement de relations de coopération dans l'application des lois

La législation et les ententes d'échange de renseignements permettent de coopérer, et souvent jusqu'au niveau mondial[2], mais ce sont les relations interorganismes et interpersonnelles dûment entretenues qui apporteront l'aisance, la confiance et le savoir organisationnel (p. ex. les points forts, les capacités juridiques et les priorités stratégiques des différentes autorités) et ouvriront les voies de communication nécessaires pour faire de la coopération une réalité. Les autorités peuvent choisir d'établir et de renforcer ce type de relations par divers moyens :

- en se regroupant et en participant activement à divers réseaux de coopération en matière de protection de la vie privée et d'application des lois (p. ex. participer à des appels mensuels et se porter volontaires afin de prendre part à des initiatives ou de siéger au sein de groupes de travail);

- en organisant des rencontres en personne ou des téléconférences pour établir des relations – en commençant peut-être par les dirigeants et d'autres cadres supérieurs des organismes pour ensuite renforcer les relations sur le plan opérationnel (p. ex. participer régulièrement à des appels opérationnels);

- en prenant part à des détachements, à des échanges d'employés ou à des activités de formation conjointes, qui permettront aux employés participants de faire bénéficier leur organisme des connaissances approfondies et mettront les gens à l'aise par rapport aux partenaires éventuels;

- en recherchant des possibilités graduelles de mettre les gens à l'aise de coopérer et de leur en donner les moyens.

Ententes d'échange de renseignements

L'échange de renseignements confidentiels ou de données personnelles est souvent crucial pour la coopération dans l'application des lois (même s'il s'agit uniquement de permettre aux autorités de faire savoir qu'elles enquêtent sur un dossier ou envisagent de le faire). Dans de nombreux cas, les parties seront en mesure d'échanger cette information, dans le respect des limites de leur législation, en vertu d'un protocole d'entente ou d'une entente n'ayant pas force exécutoire. Ce type de document énonce les attentes de chaque partie concernant les

[2] La prise en compte de valeurs communes tout au long du processus jusqu'au niveau mondial est déjà nécessaire lorsqu'on considère la façon dont chaque autorité peut mieux servir les intérêts et les droits des particuliers à l'ère du numérique et de la mondialisation. Par exemple, les différents gouvernements ont comme source d'inspiration commune des textes acceptés à grande échelle (sinon à l'échelle planétaire, sous une forme intentionnellement diversifiée comme c'est le cas à l'heure actuelle) comme l'article 12 de la *Déclaration universelle des droits de l'homme* : « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'attaques à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » ou la Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée, formulée en 2007.

situations où elles peuvent partager les renseignements. Mentionnons toutefois que pour des raisons pratiques ou légales, certaines autorités ne seront pas en mesure d'échanger des renseignements en vertu d'ententes non exécutoires, tandis que d'autres ne seront peut-être pas en situation de ratifier des ententes exécutoires.

Comme de nombreuses ententes seront dictées par des enjeux ou des besoins, une entente conclue au préalable pourra aider à gagner du temps lorsque la possibilité de coopération se présentera. En outre, elle permettra d'avoir régulièrement des discussions, ce qui aidera par le fait même à détecter les possibilités de coopération.

Les autorités peuvent opter pour l'échange de renseignements en vertu d'ententes bilatérales entre des partenaires établis. Toutefois, des ententes de portée générale, comme l'Entente de la Conférence ou l'Accord de coopération de l'APEC sur la protection transfrontière des données (Cross-border Privacy Enforcement Arrangement ou CPEA), apportent une flexibilité pour la communication multilatérale (ce qui peut s'avérer particulièrement utile pour maîtriser des risques pesant sur de nombreux pays – p. ex. une atteinte à la sécurité des données d'envergure mondiale), tout en laissant à chaque autorité participante le pouvoir de choisir les partenaires avec lesquels elle échangera des renseignements.

Les autorités peuvent être assujetties à des lois exigeant un traitement spécial des données personnelles, y compris en ce qui concerne les transferts internationaux de données personnelles. Si une ou plusieurs autorités sont soumises à de telles exigences, elles pourraient souhaiter choisir l'une des deux options suivantes :

i. convenir qu'aucune donnée personnelle ne sera échangée (en reconnaissant qu'il n'est souvent pas nécessaire d'échanger des données personnelles aux fins de la coopération dans l'application des lois);

ii. prévoir, dans l'entente même ou non, des dispositions qui énoncent de façon claire et détaillée les exigences des parties ou les limites qu'elles doivent respecter en matière d'échange de renseignements.

(Remarque : On trouvera un exemple de disposition à l'article 7 et à l'annexe I de l'Entente.)

Certaines autorités peuvent exiger le consentement de l'individu concerné avant d'échanger ses données personnelles. Lorsqu'il est impossible d'obtenir son consentement, une autorité peut décider d'aller de l'avant en retenant l'option i) ci-dessus.

La coopération reposera en grande partie sur la confiance entre les parties qui échangent des renseignements. À cette fin :

i. la partie qui communique les renseignements devrait énoncer expressément le détail de ses exigences concernant leur traitement;

ii. lorsque la loi le permet, la partie qui reçoit les renseignements devrait les traiter comme de l'information confidentielle à moins que l'autorité qui les a fournis ait expressément consenti à ce que ce ne soit pas le cas.

(Remarque : On trouvera à l'alinéa 6.1iv) de l'Entente un exemple de processus documenté pour répondre à des demandes de communication de renseignements confidentiels.)

Remarque : Lorsqu'une autorité communique des renseignements confidentiels obtenus auprès d'une organisation dans le cadre d'une enquête, elle devrait se demander s'il est approprié ou non d'informer l'organisation en question que ces renseignements ont été ou pourraient être communiqués. Il est possible qu'aucune loi ne lui impose cette obligation. Toutefois, le fait de ne pas informer l'organisation pourrait avoir des conséquences pour les secrets commerciaux (ou les renseignements commerciaux confidentiels) ou nuire aux futures relations avec celle-ci, ou avec d'autres organisations, si le dossier attire l'attention.

Avant d'échanger des renseignements, une autorité devrait effectuer une analyse attentive des exigences législatives auxquelles elle doit se conformer (p. ex. la législation ou les conventions habilitantes) pour s'assurer qu'elle comprend bien les situations et les limites en vertu desquelles elle peut partager des renseignements confidentiels et des données personnelles.

On trouvera à titre de référence des exemples de protocoles d'entente à l'**annexe B**.

Protocoles et formation sur la coopération dans l'application des lois

Les autorités peuvent envisager d'élaborer des protocoles internes et de donner une formation aux employés chargés de l'application des lois pour qu'ils aient une bonne connaissance des avantages et des options à leur disposition en matière de coopération dans l'application des lois ainsi que de leurs cadres législatifs et réglementaires respectifs. Idéalement, il s'agit de créer un climat où cette coopération leur viendra « naturellement » dans le cadre de leurs activités courantes et de les doter d'un outil de plus en matière de conformité – un climat où l'autorité sera en mesure de réagir rapidement aux possibilités de coopération lorsqu'elles se présentent.

Les questions relatives à la vie privée évoluent souvent rapidement et nécessitent une réponse rapide. Les autorités sont exhortées à répondre aux demandes de coopération en temps opportun et de manière efficace. Il peut être pertinent d'élaborer un protocole interne de coopération dans l'application des lois et de former les employés afin d'assurer une réponse rapide lorsque les possibilités de coopération se présentent.

DÉTECTION ET ÉVALUATION DES POSSIBILITÉS DE COOPÉRATION

Les autorités repéreront les possibilités de coopération par divers moyens – reportages dans les médias, plaintes du public, recherche interne, etc. Au moment de déterminer si un enjeu peut donner lieu à un type de coopération quelconque dans l'application des lois, les autorités peuvent se demander s'il présente :

- un risque pour plusieurs pays;
- un risque de préjudice appréciable ou d'incidence de grande portée;
- une question nouvelle ou stratégique en matière de protection de la vie privée.

Les autorités devront mettre au point un processus décisionnel interne afin de s'assurer qu'elles ont réfléchi comme il se doit aux possibilités de coopérer avec une autre autorité et qu'elles ont une bonne idée des lois applicables (de façon générale en vertu d'une entente avec leurs services juridiques respectifs). L'absence de compétence n'empêche pas nécessairement la coopération, selon le cadre juridique applicable et les faits inhérents au dossier, mais elle devrait être prise en compte.

L'outil d'alerte du GPEN offre aux participants une plateforme pour échanger des renseignements se rapportant à des enquêtes en cours ou éventuelles, ce qui aidera à détecter les possibilités de coopération.

Contact avec des partenaires potentiels

Il pourrait être plus facile de coopérer dans un premier temps avec des partenaires établis avec lesquels l'autorité a déjà conclu une entente d'échange de renseignements ou lorsqu'il existe un cadre juridique commun. Une fois qu'elle sera à l'aise de coopérer dans l'application des lois, l'autorité pourra juger utile d'accroître ses partenariats stratégiques.

Le ou les partenaires appropriés dans chaque cas particulier varieront en fonction des faits, mais la meilleure façon de les choisir consiste à prendre en compte les synergies pouvant découler éventuellement de la coordination – p. ex. les cas où le partenaire potentiel peut, entre autres :

- avoir lui aussi un intérêt pour l'enjeu;
- avoir accès à des éléments de preuve pertinents, par exemple des plaintes de consommateurs, ou avoir la capacité d'obtenir et de partager des documents et des dossiers pertinents;
- avoir une compétence incontestable dans le domaine (dans des cas où la compétence d'autres partenaires éventuels pourrait être mise en doute);

- être établi à proximité de la région ou du fuseau horaire où l'organisation exerce ses activités (pour faciliter la tenue de téléconférences ou la communication en personne – p. ex. une visite sur place);
- être en mesure de traiter avec l'organisation dans sa langue première;
- capacité de communiquer avec les autres partenaires dans une langue commune;
- avoir déjà établi une relation avec l'organisation;
- posséder un savoir-faire technique ou stratégique pertinent;
- détenir des pouvoirs d'application de la loi qui peuvent aider à obtenir réparation, notamment pour des individus touchés par une contravention alléguée;
- disposer de ressources pour partager la charge de travail associée à une enquête complexe.

(Remarque : Dans le monde numérique actuel, les autorités d'exécution des lois sur la protection de la vie privée se heurtent à des enjeux qui peuvent relever également de la compétence d'autorités ne s'occupant pas de la protection des données et de la vie privée. Il peut donc être approprié de nouer des liens avec d'autres partenaires éventuels, par exemple des organisations de protection des consommateurs.)

Une autorité peut en contacter une autre en utilisant :

i. la liste des contacts existants de l'organisation pour les partenaires établis;

ii. des listes de contacts à sa disposition, par exemple,
    - une liste de contacts pour l'Entente de la Conférence;
    - le GPEN (c.-à-d. la liste des contacts de l'APEC, de l'OCDE ou du Conseil de l'Europe pour l'application des lois ou le mécanisme de contact de l'outil d'alerte);
    - d'autres réseaux mondiaux, régionaux ou axés sur une langue commune (p. ex. le Plan d'action de Londres, la Commission européenne, le Groupe de travail de l'Article 29, l'Association Francophone des Autorités de Protection des Données Personnelles).

Un organisme non autorisé en vertu de la loi à communiquer des données personnelles peut commencer par communiquer des détails généraux sur l'enjeu en question. Si les deux autorités ont mutuellement intérêt à approfondir la question, elles pourront alors prendre les mesures voulues pour échanger davantage de renseignements – p. ex. conclure une entente officielle.

Dans la mesure du possible, pour éviter les délais associés à la traduction, les autorités devraient s'efforcer de communiquer avec des partenaires éventuels dans une langue comprise mutuellement.

MODÈLES DE COOPÉRATION DANS L'APPLICATION DES LOIS

La grille ci-après et le graphique de cheminement connexe serviront de base à notre analyse de la coopération dans l'application des lois.

Figure 1: Grille de coopération dans l'application des lois

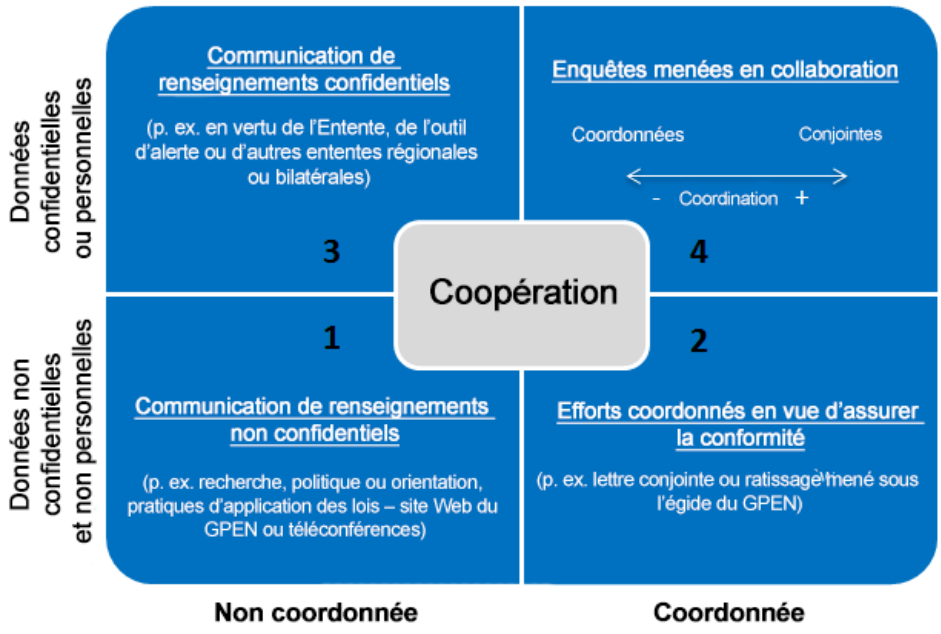
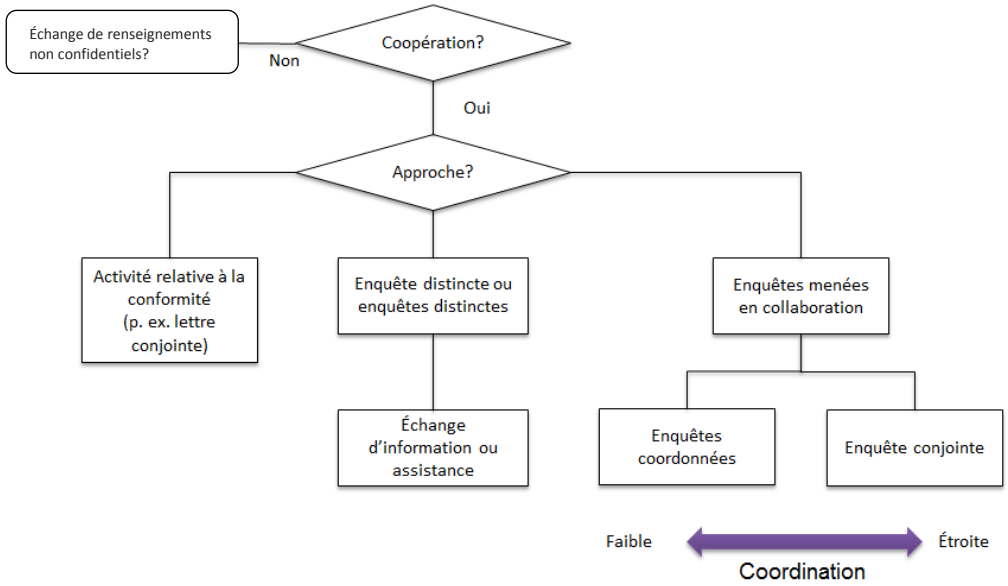


Figure 2: Graphique de cheminement de la coopération dans l'application des lois



Un modèle de coopération dans l'application des lois

La coopération dans l'application des lois peut prendre plusieurs formes :

1. **Échange de renseignements non confidentiels et d'expérience** : p. ex. politique, recherche ou pratique générales sur des questions ayant trait à l'application des lois, par l'intermédiaire de divers réseaux, plateformes Web ou réunions (en général, en dehors du cadre du présent guide).

2. **Activité concertée en matière de conformité** pouvant donner lieu ou non à l'échange de renseignements confidentiels : (p. ex. initiative thématique comme les ratissages du GPEN ou du Groupe de travail de l'Article 29 et correspondance conjointe avec certaines organisations en dehors d'une enquête officielle).

3. **Échange de renseignements confidentiels et de données personnelles et assistance** : une ou plusieurs enquêtes distinctes et unilatérales non coordonnées, appuyées par l'échange de renseignements ou une autre forme d'aide – par exemple sur la base de protocoles d'entente comme l'Entente de la Conférence ou d'une autre entente multilatérale ou bilatérale.

4. **Enquêtes menées en collaboration** (avec échange de renseignements confidentiels) pouvant comprendre divers niveaux de coordination le long d'un continuum depuis les :

    a. **Enquêtes distinctes mais coordonnées** : comportant une coordination de certains aspects de la procédure d'enquête (p. ex. collecte de renseignements ou communication publique); jusqu'aux :

    b. **Enquêtes conjointes** : comportant une coordination de la plupart ou de l'ensemble des aspects tout au long de la procédure d'enquête.

Le présent guide met l'accent sur les formes de coopération dans l'application des lois (voir ci-dessus) permettant de se pencher sur des enjeux associés à des organisations particulières, comme ceux qui pourraient donner lieu (2) à des lettres conjointes visant à assurer la conformité; (3) à un échange de renseignements confidentiels; et (4) à des enquêtes menées en collaboration.

Là encore, ces modes de coopération ne sont ni incompatibles ni exhaustifs. Par exemple :

- Des autorités pourraient dans un premier temps se contenter d'échanger des renseignements confidentiels ou d'envoyer une lettre conjointe visant à assurer la conformité, mais décider par la suite d'amorcer une enquête qui sera menée en collaboration.

- Deux autorités participant à une enquête conjointe pourraient échanger des renseignements confidentiels avec une autre autorité menant une enquête distincte sur le même enjeu.

CHOIX DE LA FORME DE COOPÉRATION APPROPRIÉE DANS L'APPLICATION DES LOIS

Aucune coopération, ou échange de renseignements non confidentiels ou d'expérience (point 1)

On encourage les autorités à privilégier la réciprocité dans leurs partenariats axés sur la coopération (le concept de l'Entente de la Conférence repose sur cette réciprocité, ce qui renforce la confiance entre les partenaires et favorise une coopération encore plus étroite). Toutefois, à moins que la législation nationale ne l'y contraigne, une autorité n'est généralement pas tenue de coopérer sur un enjeu particulier, même si elle a conclu une entente d'échange de renseignements. La coopération ne constitue pas toujours l'option appropriée (p. ex. si la loi interdit à une autorité de coopérer ou si l'autorité est incapable de coopérer en raison d'un manque de ressources). Plus précisément, l'Entente de la Conférence prend acte des situations où les autorités participantes peuvent choisir de ne pas coopérer – voir la section 5 de l'Entente, paragraphes i) à viii) (**annexe A**). Les autorités peuvent tout de même choisir d'échanger des renseignements non confidentiels ou une expérience à l'appui de leurs activités respectives d'application de la loi.

Lettre conjointe (point 2)

Au lieu d'amorcer une enquête officielle, les autorités peuvent choisir d'envoyer une lettre conjointe à une ou plusieurs organisations. De façon générale, l'envoi d'une lettre de cette nature ne nécessite pas l'échange de renseignements confidentiels ou de données personnelles.

Cette pratique peut s'avérer particulièrement appropriée lorsque le temps presse ou que les autorités pensent pouvoir obtenir des résultats en temps opportun sans consacrer les ressources nécessaires à une enquête officielle. Par exemple :

- Une violation flagrante de la loi, évidente ou apparente, touche plusieurs pays et les autorités estiment qu'elles pourront peut-être assurer la conformité en envoyant à l'organisation ou aux organisations en cause une lettre qui les incite à respecter les attentes des signataires (exigences imposées par la loi ou pratiques exemplaires). Cette mesure, que l'on peut mettre en œuvre très rapidement en utilisant des ressources très limitées, pourrait s'avérer efficace, même dans les situations où la compétence n'a pas été clairement établie. On trouvera à l'**annexe C** i) une lettre conjointe visant à assurer la conformité envoyée par sept autorités au site Web Insecam, qui diffusait en direct les images captées par des caméras; et ii) une lettre conjointe envoyée au nom de 38 autorités à Google en vue d'obtenir plus d'information sur le produit Google Glass.

- Une organisation se prépare à adopter ou a récemment adopté une nouvelle pratique ou une technologie qui suscite des préoccupations majeures concernant la protection de la vie privée. Les autorités peuvent envoyer une lettre conjointe pour i) donner à l'organisation la possibilité d'expliquer comment elle se conforme aux lois sur la protection de la vie privée ou lui demander de modifier ses pratiques en matière de protection de la vie privée dans le but d'éviter d'y contrevenir; ou ii) si la lettre est

publiée, sensibiliser le public à d'éventuels enjeux relatifs à la vie privée et montrer la solidarité qui existe entre les autorités de protection de la vie privée concernant cet enjeu.

Rédaction

Une ou deux autorités peuvent prendre l'initiative en proposant la lettre à un groupe d'autorités (p. ex. celles faisant partie d'un ou de plusieurs réseaux particuliers), en offrant de la rédiger et en faisant des suggestions, par exemple :

- les enjeux à aborder dans la lettre et l'objectif visé à terme;
- l'organisation ou les organisations auxquelles elle devrait être envoyée;
- la pertinence de rendre la lettre publique ou non.

La lettre peut mentionner ou non une violation de dispositions législatives précises, car celles-ci peuvent varier d'un pays à l'autre. Mais elle pourrait aussi y faire état de préoccupations concernant les grands principes de protection de la vie privée (p. ex. les principes de l'OCDE relatifs à l'équité dans le traitement de l'information ou de la Résolution de Madrid) ou poser des questions factuelles pour aider les signataires à mieux comprendre la pratique ou la technologie nouvelles. En outre, les signataires devraient s'entendre sur la question de savoir s'ils attendent ou non une réponse de l'organisation afin de rédiger la lettre en conséquence.

La rédaction de la lettre peut prendre de quelques jours à quelques mois selon le nombre de signataires et la contribution de chaque autorité. Si les autorités peuvent faire preuve de souplesse en ce qui a trait à la formulation, cela aide généralement les rédacteurs à finaliser la lettre rapidement en ralliant autant de signataires que possible pour avoir le maximum d'impact.

Remarque : Pour des raisons pratiques, lorsqu'ils doivent obtenir plusieurs signatures, ce qui requiert un important travail de coordination, les rédacteurs peuvent demander une version PDF du logo ou de la signature de chaque autorité pour l'intégrer avant d'envoyer la lettre conjointe au nom de tous les signataires.

Suivi

Avant de rédiger et d'envoyer la lettre, les signataires peuvent discuter des stratégies de suivi potentielles, par exemple :

i. Si la lettre vise simplement à sensibiliser l'entreprise ou le public à la protection de la vie privée, les signataires peuvent fort bien ne prendre aucune mesure de suivi ou, sous réserve des limites prévues par la loi, se contenter de rendre publique la réponse de l'organisation.
ii. Si la lettre se rapporte à un grave problème de protection de la vie privée qu'elle ne permettra pas de résoudre, une ou plusieurs autorités peuvent choisir de faire enquête sur la question (éventuellement en collaboration).
iii. En définitive, il revient à chaque autorité de déterminer les mesures qu'elle prendra en plus de l'envoi de la lettre conjointe. On suggère toutefois aux signataires de s'informer mutuellement des mesures de suivi qu'ils ont l'intention de prendre.

Échange de renseignements ou assistance (point 3)

Dans certaines situations, une autorité peut choisir de communiquer des renseignements ou de prêter assistance (en vertu du pouvoir conféré par la loi ou d'une entente) à l'appui d'une enquête en cours ou future d'une autre autorité. Les paragraphes ci-après illustrent des situations où cette approche pourrait être appropriée.

i. En vertu de sa propre procédure d'enquête (p. ex. dans le cadre d'une plainte déposée auprès de son bureau ou d'éléments de preuve recueillies au cours d'une enquête), l'**autorité A** obtient des renseignements qui se rapportent aux pratiques d'une organisation relevant de la compétence de l'**autorité B**. Elle n'a pas compétence sur l'organisation en question ou estime que l'**autorité B** serait mieux placée (en raison de l'emplacement, de la langue de communication, des pouvoirs conférés par la loi, des relations, etc.) pour faire enquête. L'**autorité A** pourrait s'adresser à l'**autorité B** pour déterminer si elle aimerait recevoir les renseignements et si elle serait en mesure de faire enquête.

ii. L'**autorité A** et l'**autorité B** font chacune enquête sur la même question ou des questions connexes, mais elles ne souhaitent pas coordonner leurs enquêtes (p. ex. pour des raisons législatives ou stratégiques). Afin d'assurer l'uniformité, ces autorités pourraient s'entendre pour échanger des éléments de preuve recueillis dans le cadre de leurs enquêtes ou de leurs suivis respectifs ou dont il est fait état dans leurs conclusions.

iii. L'**autorité A** mène une enquête et estime que l'**autorité B** pourrait détenir ou être en mesure d'obtenir des renseignements qui lui seraient utiles pour son enquête. Elle pourrait s'adresser à l'**autorité B** pour déterminer si elle est en mesure (en vertu d'un pouvoir conféré par la loi ou d'une entente – p. ex. le CPEA) de lui prêter main-forte.

De même, une autorité qui reçoit de l'information doit s'assurer de bien comprendre les fins auxquelles les renseignements reçus peuvent être utilisés et les mesures de sécurité qui s'y rattachent. Par exemple, il lui faut savoir si elle peut y faire référence dans ses constatations écrites ou les utiliser en preuve dans des procédures judiciaires.

Dans tous les cas, chaque autorité doit s'assurer qu'elle est autorisée, en vertu de la législation qui la régit, à communiquer des renseignements à une autre autorité ou à lui venir en aide. Elle doit également préciser clairement par écrit les modalités en vertu desquelles elle communique des renseignements ou apporte son aide. Une autorité autorisée par la loi à communiquer des renseignements peut choisir de le faire même si l'autorité qui les reçoit ne peut lui rendre la pareille.

De même, une autorité qui reçoit de l'information devrait s'assurer de bien comprendre les fins auxquelles les renseignements reçus peuvent être utilisés en vertu de l'entente d'échange de renseignements et des lois qui la régissent. Par exemple, il lui faut savoir si elle pourrait i) y faire référence dans des conclusions écrites, en respectant les modalités de l'entente d'échange de renseignements; ou ii) utiliser l'information reçue en preuve dans des procédures judiciaires nationales, compte tenu du type de procédure en question (p. ex. administrative, civile ou criminelle) et de toute exigence particulière en matière de preuve dans son propre cadre juridique (p. ex. équité de la procédure).

Les partenaires devraient aussi établir une compréhension commune des exigences particulières en matière de protection des données qui seront échangées. Les mesures convenues devraient tenir compte de la nature des renseignements en question et du préjudice qui pourrait résulter de leur communication non autorisée, de leur perte accidentelle ou de leur destruction. Il peut s'agir, par exemple, i) de la transmission via une plateforme existante (p. ex. outil d'alerte du GPEN) ou par courriel protégé par chiffrement ou par mot de passe; ii) de la limitation de l'accès du personnel en fonction des besoins; et iii) du stockage sous forme chiffré ou dans un classeur sous clé.

Une autorité qui a reçu des renseignements devrait les traiter comme de l'information confidentielle et, si la loi le permet, obtenir le consentement écrit de l'autorité qui les a fournis avant de les communiquer de quelque façon que ce soit.

Enquêtes menées en collaboration (point 4)

Les enquêtes menées en collaboration, qu'il s'agisse d'enquêtes « conjointes » ou d'enquêtes « distinctes mais coordonnées », offrent aux autorités participantes la possibilité d'éviter le double emploi, de tirer parti de leurs points forts relatifs et d'obtenir une coopération accrue de l'organisation ou des organisations en question pour obtenir de façon plus efficiente un plus grand impact.

Formes d'enquêtes menées en collaboration

Les enquêtes menées en collaboration donnent généralement lieu à l'échange de renseignements confidentiels, mais elles comportent également la coordination de certaines activités associées à l'application des lois. Cette collaboration proprement dite peut s'inscrire dans un continuum et faire appel à une combinaison d'approches présentées ci-après (en particulier lorsque plus de deux autorités entrent en jeu).

i. **Enquêtes distinctes mais coordonnées** : Dans d'autres situations, deux autorités ou plus peuvent déterminer qu'il serait plus efficace et efficient de mener des enquêtes distinctes mais simultanées en coordonnant certains aspects limités de la procédure d'enquête (p. ex. une analyse technique ou la publication de constatations complémentaires). Exemples de situations :

   - La loi qui la régit empêche une autorité de coordonner ses activités (p. ex. elle l'oblige à envoyer des avis distincts, à présenter des demandes de renseignements distinctes ou à formuler des constatations distinctes).
   - Les autorités en sont à des étapes différentes de la procédure d'enquête.

- Les lois ou les politiques auxquelles sont assujetties les autorités peuvent comporter des différences importantes (de sorte qu'elles voudront faire enquête sur des enjeux très différents).

ii. **<u>Enquêtes conjointes</u>** : Deux autorités ou plus peuvent s'entendre pour coordonner la plupart des aspects d'une enquête (y compris la collecte et l'analyse de renseignements, la rédaction de rapports et les communications) en ce qui a trait à une série d'enjeux convenue. L'organisation visée peut avoir l'impression qu'il s'agit d'une seule enquête. Une enquête conjointe pourrait être appropriée dans certaines situations, par exemple :

- La question présente un risque de préjudice élevé ou touche un grand nombre de personnes au sein du pays de deux autorités ou plus.
- La question semble mettre en cause une infraction aux lois de plusieurs pays.
- Chaque autorité s'assure d'avoir compétence sur l'organisation et la question.
- On observe une certaine concordance entre les lois applicables et les positions stratégiques connexes concernant les enjeux en question.
- Chaque autorité choisirait de faire enquête sur la question de façon indépendante.

Compte tenu de l'uniformité relative de la législation des différentes autorités en ce qui a trait aux mesures de sécurité, les atteintes d'envergure mondiale peuvent souvent représenter une excellence occasion pour toutes les formes de collaboration.

Questions préliminaires

Avant d'amorcer une enquête à mener en collaboration, il est généralement important que les autorités concernées se penchent sur certaines questions préliminaires. Le modèle présenté à l'annexe E pourrait s'avérer utile pour documenter ces questions.

Échange de renseignements

Les autorités visées sont-elles partie à une entente d'échange de renseignements ou la loi leur permet-elle d'échanger des renseignements confidentiels ou des données personnelles? Dans la négative, elles peuvent choisir d'adhérer à une entente existante (comme l'Entente de la Conférence) ou conclure une nouvelle entente spéciale bilatérale ou multilatérale.

Remarque : Si plus de deux autorités coordonnent leurs activités, même si elles sont toutes signataires d'une entente d'échange de renseignements, les parties devraient s'entendre sur la mesure dans laquelle les autorités peuvent s'échanger les

renseignements. (Par exemple : Les **autorités A**, **B** et **C** coordonnent leurs activités. L'**autorité A** communique des renseignements confidentiels à l'**autorité B**. Autorise-t-elle l'**autorité B** à les communiquer à l'**autorité C**?). Comme il a déjà été indiqué, si les renseignements communiqués renferment des données personnelles, les parties peuvent s'entendre ou prendre des dispositions pour qu'ils fassent l'objet de restrictions ou d'un traitement particuliers.

Approche stratégique et modalités de la collaboration

Les autorités peuvent aussi envisager de créer un document présentant une « approche stratégique » globale pour énoncer clairement leur compréhension commune des questions importantes telles que les enjeux à examiner; le rôle et les responsabilités de chaque participant; le délai d'exécution et les jalons; ainsi que les points de contact. Compte tenu des nouveaux développements qui surviennent constamment dans les enquêtes (dont bon nombre peuvent être imprévus), on pourrait faire référence à ce document évolutif, et le mettre à jour au besoin, tout au long de l'enquête afin d'assurer une compréhension commune en tout temps.

Établissement d'une compréhension commune

Les autorités devraient prendre le temps de discuter très attentivement de la possibilité de coordination pour parvenir à une compréhension commune des capacités (p. ex. savoir-faire, pouvoirs d'application de la loi ou sanctions en cas de non-conformité) et des attentes de chacune. En établissant une compréhension commune avant d'amorcer une enquête conjointe ou coordonnée, les autorités pourront i) s'assurer qu'une enquête menée en collaboration constitue en fait la stratégie optimale; et ii) s'entendre sur une stratégie de collaboration qui donnera le résultat le plus efficient et efficace. Dans le cadre d'une initiative menée en collaboration, établir des objectifs simples donne souvent plus de flexibilité pour tracer la voie en vue de les atteindre.

En particulier, les autorités qui envisagent de mener une enquête en collaboration devraient s'assurer qu'elles comprennent bien les similitudes et les différences importantes entre leurs lois respectives. Les différences n'empêchent pas nécessairement une collaboration et elles aideront même à régler nombre des questions mentionnées ci-après. Par exemple, une autorité peut juger utile d'examiner si les éléments de preuve recueillis et communiqués à une autre autorité, peut-être pour les besoins d'une forme d'enquête différente (p. ex. enquête administrative ou civile plutôt que criminelle), seraient admissibles à ses propres fins.

Détermination de la portée d'une enquête

Dans le cas d'une enquête conjointe, les autorités s'entendent généralement sur un ensemble d'enjeux communs. Idéalement, ces enjeux seraient établis en fonction du cadre de compétence de chaque autorité.

Les autorités peuvent également s'entendre pour que l'une d'entre elles fasse enquête sur un ou plusieurs enjeux supplémentaires dépassant la portée commune.

Entente sur le délai d'exécution

Comme les autorités assurent généralement une coordination en ce qui a trait aux questions d'importance stratégique pour leurs organisations respectives, le succès de cette coordination repose généralement sur l'établissement d'un consensus concernant le délai d'exécution.

En sachant que les jalons peuvent être modifiés et qu'ils devront souvent l'être, les autorités peuvent aussi envisager d'établir (et de revoir) des jalons et d'en faire état dans un document sur l'approche stratégique. Ces jalons pourraient être, par exemple : i) un avis à l'organisation; ii) la fin de l'analyse; et iii) la formulation et la publication des conclusions.

Certaines autorités sont tenues par la loi de mener à bien certaines étapes de leur enquête, ou d'en publier les conclusions, dans des délais prescrits. Dans ce cas, il faudrait faire connaître ces exigences à toutes les autorités visées afin qu'elles puissent les prendre en compte au moment d'établir les jalons.

Recensement des points de contact

Une coordination efficace requiert une étroite communication entre les autorités. Chaque autorité peut donc choisir d'établir :

a. un ou plusieurs contacts sur le plan opérationnel (p. ex. avec un enquêteur ou un analyste technique) en vue d'une communication régulière;
b. des contacts substituts afin que l'enquête ne soit pas paralysée en cas d'absence inévitable;
c. un contact avec un membre de la haute direction ou un cadre pour avoir des discussions stratégiques et donner un nouvel élan au besoin.

En raison du décalage horaire et des emplois du temps chargés, il est parfois difficile d'organiser des téléconférences ponctuelles et la correspondance par courriel peut entraîner des retards (en particulier lorsque le décalage horaire entre les autorités est important). Il peut donc être utile de prévoir des téléconférences régulières pour permettre aux autorités de se tenir mutuellement informées de leurs progrès et des développements importants dans le dossier.

Dans la mesure du possible, chaque autorité devrait désigner des interlocuteurs en mesure de communiquer dans une langue que les autres autorités comprennent. Il est possible de recourir à des services de traduction, mais cette option pourrait entraîner de longs délais.

Stratification de la participation

La stratification du degré de participation des autorités à une démarche en collaboration permet de réaliser des gains d'efficience. Par exemple, les autorités peuvent s'entendre pour que les participants à l'enquête jouent l'un des trois rôles suivants :

i. **Autorité responsable** : Les autorités peuvent convenir que l'une d'entre elles sera l'autorité responsable. Celle-ci peut i) mener sa propre enquête au lieu que plusieurs

autorités mènent chacune la leur; ou ii) dans le cas d'enquêtes distinctes mais coordonnées, assurer la liaison entre les autorités pour coordonner divers aspects de la procédure d'enquête (p. ex. collecte et communication de renseignements ou communications publiques).

Plusieurs critères sont pertinents pour déterminer quelle autorité, le cas échéant, devrait être l'autorité responsable, par exemple :

- le lieu où l'organisation est établie et le pays visé;
- un pays où un grand nombre de personnes sont touchées;
- une question constituant une priorité stratégique pour une autorité;
- une autorité dotée des ressources techniques pertinentes pour permettre de mener une enquête.

ii. **Participants actifs** : Certaines autorités peuvent juger utile i) de mener leur propre enquête « conjointe » ou « distincte mais coordonnée » ou ii) d'aider une autorité responsable concernant certains aspects de sa procédure d'enquête. Les autorités qui collaborent s'entendent généralement au départ sur une répartition des activités d'enquête entre l'autorité responsable et les participants actifs, après quoi elles réévaluent la situation tout au long de la procédure d'enquête.

iii. **Autorités intéressées** : Certaines autorités peuvent choisir de ne pas faire enquête ou de s'en remettre aux interventions d'autres autorités pour s'assurer que la question sera réglée sans qu'elles aient à consacrer des ressources à une procédure susceptible de faire double emploi. Selon ce type d'approche, une autorité intéressée pourrait apporter son soutien aux autorités qui font enquête en diffusant des communications publiques ou en communiquant des renseignements. De cette façon, elle témoignerait de son intérêt pour la question et favoriserait la conformité à l'égard des conclusions finales.

Attribution d'activités d'enquête particulières

Pour bénéficier des avantages d'une enquête menée en collaboration, les autorités devraient dans la mesure du possible tenter de répartir les tâches dans le cadre de l'enquête de manière à tirer parti de leurs points forts relatifs et des ressources disponibles pour obtenir les résultats les plus efficaces et efficients.

Collecte de renseignements et communications avec l'organisation

i. **Contacts avec l'organisation** : Dans le cas d'une enquête conjointe, les autorités peuvent choisir de désigner l'une d'entre elles comme principal point de contact pour la communication ou la correspondance régulière ou administrative avec l'organisation afin i) de limiter le double emploi ou le risque de confusion associé à plusieurs points de contact; ii) de résoudre un problème de différences linguistiques ou de décalage horaire; ou iii) de simplement répartir les responsabilités et la charge de travail connexe entre les autorités qui coordonnent leurs activités. Chaque autorité communique généralement avec ses propres plaignants au besoin.

ii. **Correspondance** : Les autorités pourraient s'entendre pour que toute la correspondance importante (p. ex. notification d'enquête, demandes initiales ou détaillées d'information, etc.) soit rédigée par une autorité qui intégrera les commentaires des autres avant de l'envoyer.

Les autorités devraient déterminer si la correspondance sera envoyée par l'une d'entre elles au nom de toutes les autorités qui coordonnent leurs activités ou séparément par chaque autorité. Si un document doit porter plusieurs signatures, il serait utile pour faciliter le processus que chaque autorité i) convienne de la méthode d'approbation de la documentation (p. ex. par courriel) et ii) fournisse une version PDF de la signature appropriée et du logo de l'autorité ainsi que du libellé du bloc de signature.

iii. **Collecte de renseignements** : Même si le principal point de contact doit relayer les questions à une organisation au nom du groupe, les autorités se concertent généralement pour formuler ces questions de manière à s'assurer qu'elles permettront d'obtenir les renseignements nécessaires à chaque autorité en fonction de son cadre législatif particulier.

Lorsque la collecte de renseignements se fait au cours d'une téléconférence ou d'une réunion, les autorités peuvent envisager de participer conjointement à la démarche au lieu de tenir plusieurs discussions unilatérales. Les interactions en direct entraînent souvent les discussions dans une direction imprévue et la présence de chaque autorité lui permet i) de s'assurer qu'elle comprend bien le matériel présenté oralement ou visuellement et ii) de poser les questions supplémentaires qui peuvent surgir.

Même si plusieurs autorités participent à la réunion, elles peuvent s'entendre à l'avance sur une liste préliminaire de questions à poser au cours de la réunion ou sur la personne qui animera le débat (généralement le principal point de contact). Cette façon de procéder aide parfois à éviter le double emploi et à s'assurer qu'il sera possible de répondre aux questions de chaque autorité dans le temps dont on dispose.

Les autorités pourraient aussi envisager de tirer parti de leurs points forts respectifs en matière de collecte d'éléments de preuve au moment de définir les responsabilités de chacune – p. ex. certaines autorités pourraient avoir le pouvoir :

- d'interroger des témoins sous serment;
- d'ordonner la production de déclarations sous serment ou de documents;
- d'entrer dans un lieu ou d'y effectuer une perquisition et de saisir des éléments de preuve; ou
- d'effectuer des enquêtes en ligne (p. ex. recherche de dispositifs ou de stockage électroniques).

Lorsqu'on recueille des éléments de preuve, il est important de tenir compte de toute exigence des différents partenaires en matière de preuve afin de s'assurer que chaque autorité qui pourrait vouloir exercer ses pouvoirs d'exécution serait en mesure d'utiliser l'information communiquée. Par exemple, certaines autorités pourraient exiger des détails sur la façon dont

l'information a été recueillie ou exiger que certaines méthodes ne soient pas utilisées (p. ex. pour se conformer aux exigences d'équité de la procédure).

Remarque : Même si les autorités choisissent de mener des enquêtes distinctes simultanées, elles peuvent se concerter pour élaborer leurs demandes de renseignements respectives afin que chacune puisse obtenir les renseignements qui pourraient être utiles à une autre. Par ailleurs, lorsqu'une autorité sait qu'une organisation a déjà fourni des réponses à une autre autorité, elle peut envisager de demander une copie de ces réponses directement à l'organisation. Cette approche permettrait d'éviter certaines complications liées à la communication de cette information en vertu d'une entente d'échange de renseignements (p. ex. transmission de documents volumineux et limitation de l'utilisation des renseignements fournis par une autre autorité).

Analyse

Lorsque la prise d'une décision concernant un enjeu nécessite une analyse en fonction de dispositions législatives sensiblement similaires (p. ex. sur la base des principes de l'OCDE relatifs à l'équité dans le traitement de l'information, de la Résolution de Madrid, ou de la Convention 108 du Conseil de l'Europe) ou des normes techniques applicables à l'évaluation des mesures de sécurité adéquates (p. ex. normes de sécurité sur les données de l'industrie des cartes de paiement), les autorités pourraient partager la responsabilité de certains aspects de l'analyse.

i. **Analyse technique** : Des enquêtes portant sur des atteintes à la sécurité des données touchant plusieurs pays ou d'autres enquêtes en lien avec la technologie pourraient offrir à une autorité la possibilité d'effectuer une analyse technique au nom d'un groupe. Une analyse technique nécessite souvent l'utilisation de matériel spécialisé ou de logiciels ou un savoir-faire que certaines autorités ne possèdent pas.

   Si les autorités souhaitent s'entendre pour que l'une d'entre elles effectue des analyses techniques particulières, elles peuvent choisir de se concerter à l'avance afin de déterminer la portée des analyses (y compris les questions techniques auxquelles il faudra répondre) ainsi que les exigences particulières en matière de preuve (p. ex. documentation du processus d'analyse ou des résultats).

   Là encore, si une autorité effectue des analyses au nom de plusieurs autorités, elle doit s'assurer qu'elle comprend bien le cadre législatif de ses partenaires.

ii. **Rédaction du rapport (analyse des politiques ou juridique)** : Les autorités qui coordonnent leurs activités peuvent néanmoins effectuer leur propre analyse et, à terme, en arriver à des conclusions différentes (même s'il est assez peu probable que des autorités coordonnant leurs activités tirent des conclusions totalement différentes, puisqu'elles devraient avoir discuté de l'enjeu en fonction de leurs cadres législatifs respectifs avant d'amorcer l'enquête menée en collaboration). Dans le cas d'une enquête conjointe, les autorités qui coordonnent leurs activités ont généralement deux options :

a. Rapport conjoint : Si les décisions sont fondées sur une analyse en vertu de lois sensiblement similaires et que les autorités peuvent dégager un consensus général concernant leurs constatations respectives, elles peuvent choisir de produire un rapport conjoint. Il est parfois difficile de s'entendre sur la formulation, mais on peut rédiger le rapport de manière à faire état des différences entre les lois des autorités et les analyses en découlant. Un rapport conjoint peut aussi offrir la possibilité de faire connaître une position unique et d'en tirer parti de manière à obtenir une plus grande coopération de la part de l'organisation et un résultat qui a plus de chances de contribuer à protéger la vie privée.

b. Rapports distincts mais coordonnés : Si une autorité doit produire son propre rapport indépendant ou que les analyses peuvent ne pas être uniformes d'un pays à l'autre (même s'il est possible que les constatations finales soient très similaires), les autorités qui coordonnent leurs activités peuvent choisir de rédiger des rapports distincts. Lorsque leurs constatations sont similaires, elles peuvent tirer parti de la force d'un message unique en publiant simultanément des rapports distincts accompagnés d'une lettre conjointe résumant leurs constatations ou les attentes à l'égard de l'organisation pour la suite des choses.

Remarque : Possibilité d'échange de renseignements : Si les autorités choisissent de ne pas coordonner leur analyse ou la rédaction de leurs rapports, elles peuvent néanmoins bénéficier de l'échange des détails de leurs analyses respectives pour améliorer leur efficience et valider leurs constatations. Cette stratégie permet parfois aux autorités i) de tirer des conclusions plus uniformes, car elles ont une compréhension commune des faits et bénéficient de leur point de vue mutuel ou ii) d'être mieux préparées à expliquer les différences entre les constatations d'un pays à l'autre.

Communications publiques

Les communications publiques offrent aux autorités la possibilité d'amplifier les résultats de leurs activités coordonnées et de bâtir la confiance entre les partenaires en s'assurant que les autres autorités sont pleinement informées et préparées à réagir à la réponse et aux demandes d'information du public qui s'ensuivront.

Le cadre législatif (ou l'approche stratégique) de chaque autorité dictera la mesure dans laquelle elle peut faire connaître au public sa participation à une enquête en cours ou les résultats d'une enquête terminée. Il est important que toutes les autorités qui coordonnent leurs activités i) comprennent, avant même d'amorcer une enquête, toutes les limites concernant la publication et ii) respectent les exigences de chaque autorité au moment de publier leurs propres déclarations publiques (p. ex. l'**Autorité A** ne peut annoncer publiquement qu'elle fait enquête sur une question, mais l'**autorité B** le peut. L'**autorité B** veut annoncer qu'elle fait enquête sur la question. En pareil cas, il est possible qu'elle doive éviter de mentionner la participation de l'**autorité A**.)

Sous réserve des restrictions susmentionnées, les autorités pourront à leur choix avoir recours à l'une des approches suivantes :

i. Communications conjointes : Les autorités peuvent diffuser des communications publiques conjointes. Il faut parfois du temps et des efforts pour s'entendre sur la formulation exacte, mais les communications conjointes témoignent d'un esprit d'unité et de solidarité entre les pays et peuvent par conséquent avoir davantage d'impact.

ii. Communications coordonnées : Si une autorité qui coordonne ses activités décide de diffuser des communications publiques distinctes de façon indépendante, il est généralement utile de transmettre le message à ses partenaires avant de le diffuser. De cette façon, i) les autres autorités pourront envoyer en même temps des messages coordonnés, qui auront ainsi davantage d'impact, ii) on pourra s'assurer que les messages ne révèlent aucun renseignement contre le gré d'un autre partenaire; ou iii) les autorités seront mieux préparées à expliquer toute différence importante entre leurs messages respectifs.

Même si la contribution d'une autorité à une enquête indépendante est limitée (p. ex. communication de renseignements, consultations sur une approche, etc.), une simple déclaration publique indiquant que « l'enquête a bénéficié de l'assistance de l'autorité X » peut véhiculer un message positif concernant la collaboration internationale.

Pouvoirs d'application de la loi

Les pouvoirs d'application de la loi conférés aux autorités varient grandement d'un pays à l'autre. Entre autres, celles-ci peuvent être habilitées à :

- imposer des amendes ou des sanctions administratives pécuniaires;
- rendre des ordonnances;
- conclure des ententes ayant force exécutoire;
- prendre des mesures administratives ou obtenir une ordonnance d'injonction;
- assurer la conformité au moyen de procédures judiciaires;
- rendre public le nom d'une organisation.

Avant d'amorcer une enquête à mener en collaboration, les autorités devraient s'assurer qu'elles connaissent bien les pouvoirs de leurs partenaires en matière d'application de la loi (ou les limites de ces pouvoirs). Chaque pouvoir peut s'avérer un moyen efficace d'assurer la conformité, d'autant plus que chaque autorité acquiert la maîtrise voulue pour tirer parti de l'ensemble unique d'outils d'application dont elle dispose. Des pouvoirs complémentaires à cet égard peuvent offrir la possibilité d'exercer des pressions plus fortes sur une organisation pour l'inciter à se conformer. C'est pourquoi il est parfois important de prendre en compte les

pouvoirs d’application de la loi respectifs au moment de choisir des partenaires aux fins d’une coordination des activités.

Par exemple, les partenaires pourraient adopter une approche en plusieurs étapes pour tirer le maximum de leurs pouvoirs respectifs. Une autorité peut commencer par rendre public le nom de l’organisation dans le but d’accélérer une conformité volontaire et de sensibiliser les intervenants. Si cette approche ne porte pas fruit, une deuxième autorité pourrait prendre le relais et intenter des poursuites judiciaires.

CONCLUSION

De plus en plus, les organisations ont tendance à établir une présence à l'échelle mondiale et elles disposent d'une technologie leur permettant de traiter un volume croissant de données personnelles. La coordination offre à l'ensemble des autorités chargées de l'application des lois sur la protection de la vie privée la possibilité de régler un problème mondial en adoptant une solution mondiale. Lorsque vous envisagez de coopérer dans l'application des lois, gardez à l'esprit quelques points clés importants :

i. Établissez et entretenez des relations avec d'autres autorités, au niveau de la haute direction et sur le plan opérationnel – ces relations jetteront les bases de la coopération.

ii. Dotez-vous à l'interne des capacités voulues pour détecter les possibilités de coopération dans l'application des lois et y donner suite – p. ex. en élaborant des protocoles, en instaurant une formation sur la coopération dans l'application des lois ou en proposant des détachements ou des échanges d'employés.

iii. Il faut généralement conclure une entente d'échange de renseignements pour coopérer dans l'application des lois – soyez proactifs et concluez à l'avance ce type d'entente pour être prêts à saisir par la suite les possibilités de coopération qui se présenteront.

iv. La forme de coopération appropriée varie d'une situation à l'autre. Les autorités peuvent obtenir des résultats concrets rien qu'en échangeant des renseignements ou en envoyant une lettre conjointe.

v. À notre époque caractérisée par l'augmentation de la circulation transfrontière, la coopération dans l'application des lois, sous toutes ses formes, permet d'obtenir de façon plus efficiente de meilleurs résultats au chapitre de la conformité. Au moment de choisir vos partenaires, envisagez les points forts des autorités qui sont complémentaires aux vôtres.

vi. Pour éviter le double emploi et tirer le maximum d'avantages d'une enquête conjointe ou coordonnée, dégagez un consensus sur un plan stratégique qui tire parti des points forts de chaque partenaire (p. ex. l'emplacement, la capacité, un savoir-faire spécial ou des pouvoirs particuliers).

vii. Le succès de la coopération repose sur la confiance. Dans la mesure du possible, les partenaires devraient s'efforcer de se tenir mutuellement pleinement informés des activités coordonnées, de respecter leurs engagements respectifs et de faire preuve de souplesse dans le but d'en arriver à un consensus.

ANNEXE A

La 36e Conférence internationale des commissaires à la protection des données et de la vie privée, à Fort Balaclava, Maurice, du 13 au 16 octobre 2014

Entente mondiale de coopération transfrontière dans l'application des lois

Table des matières

Préambule

Rappelant qu'une résolution adoptée par la Conférence de Varsovie prévoyait l'élargissement du mandat du Groupe de travail sur la coopération internationale dans l'application des lois en vue d'élaborer une approche commune pour le traitement des dossiers transfrontières et la coordination de l'application des lois, et de présenter cette approche dans un cadre multilatéral portant sur la communication d'information liée à l'application des lois, notamment sur la façon dont cette information doit être traitée par ceux qui la reçoivent;

Prenant acte qu'un phénomène mondial nécessite une intervention mondiale et que la création de stratégies et d'outils efficaces pour éviter les doubles emplois, faire une utilisation plus efficace des ressources limitées et améliorer l'efficacité de l'application de la loi dans les situations où les atteintes à la vie privée et à la sécurité des données transcendent les frontières nationales est dans l'intérêt des autorités[1], des individus, des gouvernements et des entreprises;

Conscients qu'il est de plus en plus apparent que l'augmentation de la circulation transfrontière des données et que les pratiques des organisations nationales et multinationales associées à cette circulation peuvent rapidement porter atteinte à la vie privée et à la protection des données personnelles d'un très grand nombre de personnes dans le monde et que, par conséquent, cette augmentation de la circulation transfrontière de données devrait s'accompagner d'une meilleure communication de l'information entre autorités d'exécution des lois sur la protection des données et de la vie privée et d'une coopération internationale accrue dans l'application des lois, et que cette communication et cette coopération sont essentielles pour protéger la vie privée et les données et servir ainsi un intérêt public important;

Tenant compte du fait que plusieurs autorités ont à plusieurs occasions fait enquête en même temps sur les mêmes pratiques ou atteintes;

Rappelant les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 du Conseil de l'Europe), en particulier les dispositions sur l'entraide énoncées au chapitre IV;

Rappelant que la *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée* (2007) conseille aux pays membres de coopérer au niveau international pour faire appliquer les lois sur la protection des données et de la vie privée et de prendre les mesures voulues afin :

- d'améliorer leurs cadres nationaux d'application des lois sur la protection des données et de la vie privée afin de faciliter la coopération transfrontière dans le respect des lois nationales;

- d'avoir recours à l'assistance mutuelle pour assurer l'application des lois sur la protection des données et de la vie privée, notamment par la notification, la transmission des plaintes, l'aide aux enquêtes et la communication d'information sous réserve des mesures de sécurité appropriées;

- d'engager les intervenants pertinents aux discussions et activités visant à renforcer la coopération dans l'application des lois sur la protection des données et de la vie privée;

Rappelant que les résolutions adoptées lors des Conférences internationales des commissaires à la protection des données et de la vie privée précédentes et la Déclaration de Montreux encourageaient notamment les autorités à redoubler d'efforts pour appuyer la coopération internationale dans l'application des lois et à travailler avec les organisations internationales afin de renforcer la protection des données à l'échelle mondiale;

Faisant fond sur les progrès considérables accomplis au cours des dernières années aux niveaux régional et international pour améliorer les accords portant notamment sur la coopération transfrontière dans l'application des lois sur la protection des données et de la vie privée;

Reconnaissant que la coopération transfrontière dans l'application des lois peut prendre différentes formes; elle peut avoir lieu à différents niveaux (national, régional ou international), être de différents types (coordonnée ou non) et porter sur plusieurs activités (communication de pratiques exemplaires, ratissages d'Internet, enquêtes coordonnées ou mesures concertées d'application des lois menant à des peines ou à des sanctions); toutefois, quelle que soit la forme de cette coopération, son succès repose sur l'instauration d'une culture de communication proactive et pertinente de l'information, qui peut être confidentielle ou non et renfermer ou non des données personnelles, et sur une coordination appropriée des activités d'application des lois;

Encourageant toutes les autorités à utiliser et à perfectionner les plateformes de coopération et les mécanismes d'application de la loi connexes et à aider à optimiser l'efficacité de la coopération transnationale dans l'application de la loi;

Concluant qu'il faut adopter une approche multilatérale pour intervenir efficacement à la suite d'atteintes à la sécurité des données et à la vie privée qui touchent plusieurs territoires de ressort et que l'on a donc grand besoin, pour contrer ces atteintes, de mécanismes appropriés facilitant la communication d'information confidentielle concernant l'application de la loi et la coordination entre les autorités chargées de son application;

Conséquemment, les autorités sont fortement encouragées à adhérer à la présente entente et à s'engager à respecter ses dispositions, notamment celles régissant la confidentialité et la protection des données, quand elles participent à des activités transfrontières d'application des lois.

1. Définitions

Les définitions suivantes s'appliquent pour les besoins de la présente entente :

Coopération dans l'application des lois – Expression générale faisant référence à des autorités qui collaborent pour appliquer les lois sur la protection des données et de la vie privée.

Application concertée des lois – Type particulier de coopération dans l'application des lois en vertu de laquelle deux ou plusieurs autorités concertent leurs activités en vue de faire respecter les lois sur la protection des données et de la vie privée sur leurs territoires respectifs.

Lois sur la protection des données et de la vie privée – Ensemble des lois d'un territoire de ressort dont l'application a pour effet de protéger les données personnelles.

Autorité d'exécution de la loi sur la protection des données et de la vie privée (« autorité[2] ») – Tout organisme public ayant la responsabilité d'appliquer les lois sur la protection de la vie privée ou des données et détenant le pouvoir de faire enquête ou de prendre des mesures d'application des lois.

Demande d'assistance – Requête adressée par une partie à une ou plusieurs autres parties en vue de coopérer et de coordonner l'application d'une loi sur la protection des données et de la vie privée, entre autres :

i. le renvoi d'une question liée à l'application d'une loi sur la protection des données et de la vie privée;

ii. une demande de coopération dans l'application d'une loi sur la protection des données et de la vie privée;

iii. une demande de coopération dans une enquête au sujet d'un manquement allégué à une loi sur la protection des données et de la vie privée;

iv. le transfert d'une plainte alléguant un manquement à une loi sur la protection des données et de la vie privée.

Partie – Autorité signataire de la présente entente.

Comité – Comité de direction de la Conférence internationale des commissaires à la protection des données et de la vie privée.

Plaignant – Toute personne ayant déposé auprès de l'autorité une plainte alléguant un manquement à une loi sur la protection des données et de la vie privée.

2. Objet

La présente entente a pour objet de favoriser la protection des données par les organisations qui traitent des données personnelles dans plusieurs territoires de ressort. Elle encourage et facilite la coopération entre toutes les autorités grâce à la communication d'information, en particulier de l'information confidentielle concernant l'application des lois en lien avec des enquêtes éventuelles ou en cours, et s'il y a lieu, l'entente régit en outre la coordination des activités d'application de la loi par ces autorités pour leur permettre d'utiliser leurs ressources limitées de façon aussi efficiente et efficace que possible.

3. Finalité

La présente entente vise à réaliser sa finalité en atteignant les objectifs suivants :

i. énoncer les principales dispositions à appliquer pour communiquer l'information concernant l'application des lois, notamment l'utilisation de cette information par les parties qui la reçoivent;

ii. énoncer les principales dispositions à appliquer pour communiquer l'information concernant l'application des lois, notamment l'utilisation de cette information par les parties qui la reçoivent;

iii. encourager les parties à s'engager dans une coopération transfrontière en faisant appel à la communication d'information concernant l'application de la loi et, s'il y a lieu, à la mise en commun de leur savoir, leur expertise et leur expérience susceptibles d'aider d'autres parties à aborder les questions d'intérêt commun;

iv. encourager les parties à appuyer la création de plateformes sécurisées pour la communication électronique de l'information et à s'en servir pour s'échanger l'information concernant l'application des lois, en particulier l'information confidentielle concernant les activités éventuelles ou en cours d'application des lois.

4. Nature de l'entente

La présente entente énonce les engagements des parties à l'égard de la coopération transfrontière dans l'application des lois, en particulier au chapitre de la réciprocité, de la confidentialité, de la protection des données et de la coordination.

L'entente NE VISE PAS :

i. à remplacer les conditions ou mécanismes nationaux et régionaux existants régissant la communication de l'information ni à contrecarrer les accords similaires conclus par l'entremise d'autres réseaux;

ii. à créer des obligations juridiquement contraignantes ni à modifier des obligations existantes découlant d'autres ententes ou du droit international ou national;

iii. à empêcher une partie de coopérer avec d'autres parties, ou avec des autorités qui ne sont pas parties à la présente, en vertu d'autres lois, accords, traités ou ententes (juridiquement contraignants ou non);

iv. à créer des obligations ou des attentes de coopération qui vont au-delà de l'autorité ou de la compétence d'une partie;

v. à contraindre les parties à collaborer dans le cadre d'activités d'application de la loi, notamment à fournir de l'information confidentielle ou non qui renferme ou non des données personnelles.

5. Principe de réciprocité

Toutes les parties coopéreront dans la mesure du possible avec les autres parties et leur viendront en aide dans le cadre des activités d'application transfrontière des lois, notamment en répondant aux demandes d'assistance dans les meilleurs délais possible.

Quand ils communiquent des données et de l'information concernant l'application des lois en vertu de la présente entente, les parties devraient indiquer par écrit qu'elles le font conformément aux modalités de cette entente. Les parties qui reçoivent une demande d'assistance devraient en accuser réception dans les meilleurs délais, de préférence dans les deux semaines suivant réception de la demande.

Avant d'effectuer une demande d'assistance auprès d'une autre partie, la partie demanderesse devrait effectuer une vérification préliminaire interne pour s'assurer que la demande s'inscrit dans le champ d'application et l'objet de la présente entente et qu'elle n'impose aucun fardeau excessif à l'autre partie. Si elle le souhaite, une partie peut limiter sa coopération dans l'application transfrontière de la loi, notamment dans les situations suivantes :

i. la question ne relève pas de son autorité ou de sa compétence;

ii. la question ne constitue pas un acte ou une pratique au sujet de laquelle elle peut faire enquête ou au sujet de laquelle ses lois nationales peuvent être appliquées;

iii. les ressources sont limitées;

iv. la question est incompatible avec d'autres priorités ou obligations juridiques;

v. la question ne présente pas un intérêt mutuel;

vi. la question n'entre pas dans le champ d'application de la présente;

vii. un autre organisme serait mieux désigné pour s'occuper de la question;

viii. toute autre situation qui empêcherait une partie de coopérer.

Si une partie refuse ou limite sa coopération, elle devrait en indiquer les raisons par écrit à la partie qui l'a sollicitée, dans la mesure du possible dans les quatre semaines suivant réception de la demande d'assistance.

6. Principe de confidentialité

6.1 Sous réserve du paragraphe 6.2, les parties assurent la confidentialité de toute information reçue d'autres parties en vertu de la présente entente :

i. en respectant le caractère confidentiel de toute information reçue ou de toute demande d'assistance au titre de la présente entente, y compris le fait qu'une autre partie envisage de faire enquête, a entrepris une enquête ou mène actuellement une enquête et au besoin, en

prenant des arrangements supplémentaires pour se conformer aux exigences légales nationales de la partie qui envoie des renseignements;

ii. en ne communiquant pas à un tiers l'information obtenue d'autres parties, notamment à d'autres autorités nationales ou à d'autres parties sans le consentement écrit de la partie ayant fourni l'information en vertu de la présente entente;

iii. en limitant l'utilisation de cette information aux fins pour lesquelles elle a été communiquée au départ;

iv. si une partie reçoit d'un tiers (par exemple un individu, un organisme judiciaire ou un autre organisme d'exécution de la loi) une demande de communication d'information confidentielle reçue d'une autre partie en vertu de la présente entente, elle doit :

   a. s'opposer à la demande, ou s'efforcer de la limiter le plus possible;
   b. respecter le caractère confidentiel de l'information en question;
   c. informer sans délai la partie ayant fourni l'information et à chercher à obtenir son consentement à la communication de l'information en question;
   d. informer la partie ayant fourni l'information de l'existence de lois nationales qui exigent néanmoins la communication, si la partie ayant fourni l'information refuse de consentir à la communication;

v. en cas de retrait de l'entente, en respectant le caractère de toute information confidentielle communiquée par une autre partie en vertu de la présente entente ou encore, avec l'accord mutuel des autres parties, en retournant l'information, en la détruisant ou en l'effaçant;

vi. en veillant à ce que toutes les mesures techniques et organisationnelles voulues soient prises pour protéger toute information fournie en vertu de la présente entente, notamment en retournant ou en traitant l'information (conformément à la législation nationale dans la mesure du possible) dans le respect des conditions de consentement de la partie ayant fourni l'information.

6.2 S'il est possible que des obligations juridiques nationales empêchent une partie de respecter l'un des points des alinéas 6.1i) à vi), il doit en informer au préalable les parties ayant fourni l'information.

7. Principes de protection des données et de la vie privée

Selon les parties ou l'activité d'application de la loi en question, il pourrait être nécessaire de communiquer des renseignements personnels. Toutefois, pour respecter les principes reconnus en matière de protection des données et de la vie privée, la communication de renseignements personnels devrait se limiter le plus possible aux situations où cette communication est nécessaire pour garantir une application efficace de la loi sur la protection de la vie privée et des données. Toutes les parties à l'entente qui communiquent ou reçoivent des données personnelles feront de leur mieux pour respecter leurs mesures de sécurité mutuelles visant à protéger les données. Les autorités reconnaissent cependant que ces efforts ne suffisent pas toujours pour permettre la communication de renseignements personnels.

Dans ce cas, si la partie qui communique des renseignements personnels a besoin de mesures de sécurité particulières visant à protéger les données, elle devrait :

- demander aux autres parties de lui donner l'assurance qu'elles se conformeront aux exigences énoncées à l'annexe I;

ou prévoir d'autres ententes entre la partie qui communique les données personnelles et la partie qui les reçoit de manière à assurer le respect intégral des exigences de chaque partie concernant la protection des données et de la vie privée. Les parties doivent indiquer au Comité si elles s'engagent à respecter les exigences énoncées à l'annexe I ou lui faire part d'autres arrangements tel qu'il est susmentionné. En principe, cet avis devrait être donné au moment de présenter un avis d'intention de participer conformément à l'article 13 ou, en tout état de cause, avant de recevoir des données personnelles d'une autre partie en vertu de la présente entente. Une liste des parties, y compris leurs avis initiaux et mis à jour concernant l'annexe I et tout autre arrangement tel qu'il est susmentionné, sera mise à la disposition de toutes les parties.

8. Principes de coordination

Les parties feront de leur mieux pour coordonner leurs activités d'application transfrontière des lois. Les principes qui suivent ont été établis en vue de coordonner l'application transfrontière des lois sur la protection de la vie privée ou des données :

i. Détermination des activités qui se prêteraient à une coordination

   a. Les autorités devraient cerner les questions ou les incidents qui se prêteraient à une coordination et rechercher activement les possibilités de coordonner leurs activités lorsque c'est possible et bénéfique.

ii. Évaluation des possibilités de participation

   a. Les autorités devraient évaluer attentivement, au cas par cas, la pertinence de participer à une application de la loi coordonnée et communiquer clairement leur décision aux autres autorités.

iii. Participation à des actions coordonnées

   a. Les autorités devraient évaluer attentivement, au cas par cas, la pertinence de participer à une application de la loi coordonnée et communiquer clairement leur décision aux autres autorités.

iv. Facilitation de la coordination

   a. Les autorités devraient se préparer à l'avance à participer à des actions coordonnées.

v. Direction d'une action coordonnée

a. Les autorités qui dirigent une action coordonnée devraient conclure des ententes pratiques qui simplifient la coopération et appuient ces principes.

Les parties peuvent se reporter au Cadre de coordination internationale de l'application des lois pour un complément d'information au sujet de ces principes.

9. Résolution des problèmes

Tout différend entre les parties en lien avec la présente entente devrait de préférence être réglé par voie de discussion entre leurs personnes-ressources désignées et, à défaut d'un règlement dans un délai raisonnable, entre les premiers dirigeants des parties.

10. Répartition des coûts

Chaque partie prend à sa charge ses propres coûts associés à la coopération, conformément à la présente entente.

Les parties peuvent convenir de partager ou de transférer les coûts d'une coopération en particulier.

11. Restitution des éléments de preuve

Les parties renvoient les éléments dont ils n'ont plus besoin si la partie qui les a fournis a demandé par écrit au moment de leur communication qu'ils lui soient renvoyés. Si la partie ayant fourni les éléments ne demande pas qu'ils lui soient renvoyés, l'autre partie en dispose selon une méthode prescrite par la partie qui les a fournis ou, si cette dernière n'a précisé aucune méthode, selon une méthode sécuritaire, dans les meilleurs délais possible après que les éléments ne sont plus nécessaires.

12. Critères d'admissibilité

Toute autorité peut présenter au Comité un avis d'intention indiquant qu'elle s'engage à participer à la présente entente :

i. en tant que membre, si elle est un membre agréé de la Conférence internationale des commissaires à la protection des données et de la vie privée (la Conférence) et donc répond aux exigences d'admissibilité énoncées à l'article 5.1 des règles et procédures de la Conférence, notamment l'exigence concernant une autonomie et une indépendance appropriées;

ii. ou en tant que partenaire, même si elle n'est pas un membre accrédité de la Conférence, si
   a. elle représente un État signataire de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108);
   b. ou elle est membre du Global Privacy Enforcement Network (GPEN);
   c. ou elle participe à l'Accord de coopération de l'APEC sur la protection transfrontière des données (Cross-border Privacy Enforcement Arrangement ou CPEA);
   d. ou elle est membre du Groupe de travail Article 29.

Le Comité conservera une liste actualisée de toutes les autorités qui se sont engagées à participer à la présente entente et de toutes celles qui se seront engagées à respecter l'annexe I. Toutes les parties devraient avoir facilement accès à cette liste.

13. Rôle du comité de direction de la conférence internationale

Le Comité :

a. reçoit les avis d'intention de participer à l'entente ou de s'en retirer;

b. reçoit les avis d'engagement à l'annexe I ou autres arrangements comme il est mentionné à l'article 7;

c. examine ces avis pour vérifier que l'autorité peut être partie à l'entente;

d. examine la mise en œuvre de l'entente trois ans après son entrée en vigueur et présente ses conclusions à la Conférence internationale;

e. fait connaître l'entente;

f. recommande à la Conférence internationale, après avoir dûment tenu compte des renseignements, que la participation d'une partie soit suspendue ou encore, dans les cas les plus graves de non-conformité aux exigences énoncées dans l'entente — et donc de bris du lien de confiance que l'entente a instauré entre les parties — recommande à la Conférence internationale que la partie soit exclue de l'entente.

14. Retrait de l'entente

Une partie peut se retirer de l'entente en donnant au Comité un préavis écrit d'un mois.

Dans les plus brefs délais après avoir informé le Comité de son intention de se retirer de l'entente, une partie prendra toutes mesures raisonnables pour informer les autres parties de son retrait. Elle devrait afficher cette information sur son propre site Web pendant qu'elle participe encore à l'entente et durant une période raisonnable après son retrait.

Une partie qui participe activement à une activité d'application transfrontière de la loi en vertu de la présente entente devrait s'efforcer de s'acquitter de ses obligations en lien avec cette activité avant de se retirer.

Indépendamment du retrait d'une partie, toute information reçue en vertu de la présente entente demeure assujettie au principe de confidentialité énoncé à l'article 6, aux principes de protection des données énoncés à l'article 7 et, s'il y a lieu, à l'annexe I de l'entente.

15. Entrée en vigueur

Le Comité acceptera les avis d'intention à partir de la date de la 37e Conférence, et l'entente entrera en vigueur dès qu'elle comptera au moins deux parties.

Les autorités deviendront des parties à l'entente lorsque le Comité leur aura signifié qu'elles sont acceptées.

Annexe I

1) En vertu de l'article 7 de la présente entente, les engagements prévus dans la présente annexe pourraient être appropriés pour permettre l'échange de données personnelles.

Toutefois, la présente annexe n'écarte pas les situations où les lois sur la protection des données et de la vie privée d'une partie exigent des mesures de sécurité supplémentaires dont doivent convenir les parties avant toute communication de renseignements personnels.

Les parties qui communiquent des données personnelles et qui se sont engagées à respecter la présente annexe doivent respecter les conditions suivantes dans la mesure où elles sont en mesure de le faire :

i. limiter la communication de données personnelles aux situations qui l'exigent absolument et, quoi qu'il en soit, communiquer uniquement des données personnelles pertinentes et non excessives compte tenu de la fin précise pour laquelle elles sont communiquées. En tout état de cause, les données personnelles ne doivent pas être communiquées à grande échelle ni d'une façon structurelle ou répétitive;

ii. veiller à ce que les données personnelles communiquées d'une partie à une autre ne soient pas utilisées par la suite à des fins incompatibles avec la fin pour laquelle elles ont été communiquées au départ;

iii. veiller à ce que les données personnelles communiquées d'une partie à une autre soient exactes et, au besoin, tenues à jour;

iv. n'adresser aucune une demande d'assistance à une autre partie au nom d'un plaignant sans le consentement explicite de ce dernier;

v. informer l'intéressé : a) de l'objet de la communication; b) de la possibilité que la partie ayant reçu les données personnelles les stocke ou les traite ultérieurement; c) de l'identité de la partie qui reçoit les données personnelles; d) des catégories de données visées; e) du droit de consulter et de corriger les données; f) de toute autre information nécessaire pour assurer un traitement équitable. Ce droit peut être limité au besoin pour protéger l'intéressé ou les droits et libertés d'autres personnes;

vi. veiller à ce que l'intéressé ait le droit de consulter ses données personnelles, de les corriger s'ils se révèlent inexacts et de s'opposer à la communication, au stockage ou à tout autre traitement des données personnelles qui le concernent. Ces droits peuvent être limités au besoin pour protéger l'intéressé ou les droits et libertés d'autres personnes; le droit de s'opposer peut être davantage limité si l'exercice de ce droit risque de porter préjudice à l'intégrité de la mesure d'application entre les participants, ou s'il compromet d'autres obligations juridiques nationales; si des données personnelles sensibles sont communiquées et font l'objet de tout autre traitement, veiller à ce que des mesures de sécurité supplémentaires soient mises en place, par exemple, exiger le consentement explicite de l'intéressé;

vii. sur réception de données personnelles, prendre toutes les mesures de sécurité techniques et organisationnelles adaptées aux risques que posent la communication, l'utilisation ultérieure ou le stockage de ces données. Les parties doivent également veiller à ce que toute organisation traitant des données en leur nom prenne des mesures de sécurité et que cette organisation n'utilise pas ou ne stocke pas de renseignements personnels sauf si la partie qui les a reçus lui en donne l'instruction;

viii. veiller à ce que toute entité à laquelle la partie ayant reçu les données les lui transfère par la suite soit également assujettie aux mesures de sécurité énoncées ci-dessus;

ix. si un tiers (par exemple un individu, un organisme judiciaire ou une autre autorité de la loi) demande à une partie de lui communiquer des données personnelles reçues d'une autre partie en vertu de la présente entente, veiller à ce que la partie ayant reçu la demande :

   a. s'oppose à la demande, ou s'efforce de la limiter le plus possible;
   b. informe sans délai la partie ayant fourni les données et cherche à obtenir son consentement à la communication de l'information en question;
   c. si la partie ayant fourni ces données refuse de consentir à la communication, l'informer si des lois nationales exigent la communication.

x. s'assurer que des mécanismes sont en place pour surveiller la conformité à ces mesures de sécurité et offrir à l'intéressé un recours approprié en cas de non-conformité.

2) Dans la présente annexe, « données personnelles sensibles » désigne :

a. des données qui concernent l'intimité du plaignant; ou

b. des renseignements susceptibles de donner lieu, en cas d'utilisation abusive :

   i. à une discrimination illicite ou arbitraire; ou
   ii. à de graves risques pour l'intéressé.

En particulier, les données personnelles qui peuvent révéler des aspects tels l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ainsi que les données relatives à la santé ou à la vie sexuelle sont considérées comme des données sensibles. Les lois nationales applicables peuvent prévoir d'autres catégories de données sensibles répondant aux conditions énoncées dans le paragraphe précédent.

---

[1] Afin d'éviter toute ambiguïté, l'expression « autorités » ou « autorités d'exécution des lois sur la protection des données et de la vie privée » englobe pour les besoins du présent document les autorités de protection des données personnelles.

[2] Afin d'éviter toute ambiguïté, l'expression « autorités » ou « autorités d'exécution des lois sur la protection des données et de la vie privée » englobe pour les besoins du présent document les autorités de protection des données personnelles.

ANNEXE B

Original disponible en anglais seulement.

MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES FEDERAL TRADE COMMISSION AND THE DUTCH DATA PROTECTION AUTHORITY ON MUTUAL ASSISTANCE IN THE ENFORCEMENT OF LAWS PROTECTING PERSONAL INFORMATION IN THE PRIVATE SECTOR

The United States Federal Trade Commission ("FTC") and the Dutch Data Protection Authority (“College bescherming persoonsgegevens” or “CBP”), (collectively, "the Participants"),

RECOGNIZING the nature of the modern global economy, the increase in the flow of personal information across borders, the increasing complexity and pervasiveness of information technologies, and the resulting need for increased cross-border enforcement cooperation;

RECOGNIZING that the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, the Global Privacy Enforcement Network’s Action Plan, resolutions of the International Conference of Data Protection and Privacy Commissioners, and the APEC Privacy Framework call for the development of cross-border information-sharing mechanisms and enforcement cooperation arrangements; and that such information sharing and enforcement cooperation are essential elements to ensure privacy and data protection compliance, serving an important public interest;

RECOGNIZING that the U.S. Federal Trade Commission Act, 15 U.S.C. § 41 et seq., as amended by the U.S. SAFE WEB Act, authorizes the FTC to share information with law enforcement authorities from other countries under appropriate circumstances;

RECOGNIZING that subsection 1 and 2 of Section 2:5 of the Dutch General Administrative Law Act (de Algemene wet bestuursrecht) provide that a Dutch public body may disclose confidential information to (a) person(s) or organization who is involved in the execution of the task of this Dutch public body if this is necessary to fulfill the supervisory task of the Dutch public body and the confidentiality of the information is maintained;

RECOGNIZING that the CBP is the designated authority in the Netherlands for the purposes of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (which was opened for signature on 28th January 1981) and is the supervisory authority in the Netherlands for the purposes of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

RECOGNIZING that the Participants each have functions and duties with respect to the protection of personal information in their respective countries;

RECOGNIZING that the Participants have worked together in connection with several international initiatives related to privacy;

REGOGNIZING that the Participants have cooperated in the context of several international networks, including the Global Privacy Enforcement Network, and the International Conference of Data Protection and Privacy Commissioners; and

RECOGNIZING that the Participants would not be able to provide assistance to the other if such assistance is prohibited by their respective national laws, such as privacy, data security, or confidentiality laws; or enforcement policies.

HAVE REACHED THE FOLLOWING UNDERSTANDING:

I. **Definitions**

For the purposes of this Memorandum,

A. "Applicable Privacy Law" means the laws identified in Annex 1, which may be revised by mutual consent of the Participants, including any regulations implemented pursuant to those laws, the enforcement of which has the effect of protecting personal information.

B. "Covered Privacy Violation" means practices that would violate the Applicable Privacy Laws of one Participant's country and that are the same or substantially similar to practices prohibited by any provision of the Applicable Privacy Laws of the other Participant's country.

C. “Person” means any natural person or legal entity, including corporations, unincorporated associations, or partnerships, established,

existing under or authorized by the laws of the United States, its States, or its Territories, or the laws of the Netherlands.

D. "Request" means a request for assistance under this Memorandum.

E. "Requested Participant" means the Participant from which assistance is sought under this Memorandum, or which has provided such assistance.

F. “Requesting Participant” means the Participant seeking assistance under this Memorandum, or which has received such assistance.

II. **Objectives and Scope**

A. This Memorandum of Understanding sets forth the Participants’ intent with regard to mutual assistance and the exchange of information for the purpose of investigating, enforcing and/or securing compliance with Covered Privacy Violations. The Participants do not intend the provisions of this Memorandum of Understanding to create legally binding obligations under international or domestic laws.

B. The Participants understand that it is in their common interest to:

1. cooperate with respect to the enforcement of the Applicable Privacy Laws, including sharing complaints and other relevant information and providing investigative assistance;

2. facilitate research and education related to the protection of personal information;

3. facilitate mutual exchange of knowledge and expertise through training programs and staff exchanges;

4. promote a better understanding by each Participant of economic and legal conditions and theories relevant to the enforcement of the Applicable Privacy Laws; and

5. inform each other of developments in their respective countries that relate to this Memorandum.

C. In furtherance of these common interests, and subject to Section IV, the Participants intend to use best efforts to:

1. share information, including complaints and other personally identifiable information, that a Participant believes would be relevant to investigations or enforcement proceedings regarding Covered Privacy Violations of the Applicable Privacy Laws of the other Participant's country;

2. provide investigative assistance in appropriate cases, including obtaining evidence under the Participants' respective legal authorities on behalf of the other Participant;

3. exchange and provide other relevant information in relation to matters within the scope of this Memorandum, such as information relevant to consumer and business education; government and self-regulatory enforcement solutions; amendments to relevant legislation; technological expertise, tools or techniques; privacy and data security research; and staffing and resource issues;

4. explore the feasibility of staff exchanges and joint training programs;

5. coordinate enforcement against cross-border Covered Privacy Violations that are priority issues for both Participants;

6. participate in periodic teleconferences to discuss ongoing and future opportunities for cooperation; and

7. provide other appropriate assistance that would aid in the enforcement against Covered Privacy Violations.

III. **Procedures Relating to Mutual Assistance**

A. Each Participant is to designate a primary contact for the purposes of requests for assistance and other communications under this Memorandum.

B. If a Participant requests assistance for matters involved in the enforcement of Applicable Privacy Laws, then Participants understand that:

1. requests for assistance are to include sufficient information to enable the Requested Participant to determine whether a request relates to a Covered Privacy Violation and to take action in appropriate circumstances. Such information may include a description of the facts underlying the request and the type of assistance sought, as well as an indication of any special precautions that should be taken in the course of fulfilling the request;

2. requests for assistance are to specify the purpose for which the information requested will be used;

3. consistent with Section V.A., a request for assistance certifies that, subject to any relevant applicable legal restrictions in its own jurisdiction on its ability to do so, the Requesting Participant is to maintain confidentiality in respect of:

- each request for assistance,
- the existence of any investigation related to the request,
- all materials related to each request, and
- all information and material provided in response to each request,

unless otherwise decided; and,

4. prior to requesting assistance, Participants should perform a preliminary inquiry to ensure that the request is consistent with the scope of this Memorandum.

C. Participants should use their best efforts to resolve any disagreements related to cooperation that may arise under this Memorandum through the contacts designated under Section III.A, and, failing resolution between the designated contacts in a reasonably timely manner, by discussion between appropriate senior officials designated by the Participants.

IV. **Limitations on Assistance**

A. The Requested Participant may exercise its discretion to decline the request for assistance, or limit or condition its cooperation, including where it is outside the scope of this Memorandum, or more generally, where it would be inconsistent with domestic laws, or important interests or priorities.

B. The Participants recognize that it is not feasible for a Participant to offer assistance to the other Participant for every Covered Privacy Violation.

Accordingly, the Participants intend to use best efforts, as outlined in Section II, to seek and provide cooperation focusing on those Covered Privacy Violations most serious in nature, such as those that cause or are likely to cause damage or distress to a significant number of persons, and those otherwise causing substantial damage or distress, especially if this concerns both countries.

C. If the Requested Participant is unable to offer full assistance or declines assistance, it should explain the reasons why.

D. Participants intend, in so far as they are able and are allowed by their domestic laws, to share confidential information pursuant to this Memorandum only to the extent that it is necessary to fulfill the purposes set forth in Section II.

V. **Confidentiality, Privacy, and Limitations on Use**

A. Subject to any restrictions imposed by their respective national laws, to the fullest extent possible, each Participant certifies the confidentiality of information to be shared under this Memorandum. The certification of confidentiality applies not only to the shared information, but also to the existence of an investigation to which the information relates. The Participants are to treat the shared information, the existence of the investigation to which the information relates, and any requests made pursuant to this Memorandum as confidential, and so far as they are able, not further disclose or use this information for purposes other than those for which it was originally shared, without the prior written consent of the Requested Participant.

B. Notwithstanding Section V.A., it is understood that:

1. A Participant may disclose information provided pursuant to this Memorandum in response to a formal request from a Participant country's legislative body or an order issued from a court with proper jurisdiction in an action commenced by the Participant or its government.

2. Material obtained in connection with the investigation or enforcement of criminal laws may be used for the purpose of investigation, prosecution, or prevention of violations of either Participant's country's criminal laws.

C. Each Participant is to use best efforts to safeguard the security of any information received under this Memorandum and respect any safeguards decided by the Participants. In the event of any access to, or disclosure of, the information not authorized by a Participant, the Participants are to take all reasonable steps to prevent a recurrence of the event and are to notify the other Participant of the occurrence.

D. Where a Participant receives an application by a third party for disclosure of confidential information or materials received from a Requested Participant, the Requesting Participant should notify the Requested Participant forthwith and seek to obtain that Participant's consent to the release of the information or – if the Requested Participant does not agree with the disclosure – oppose, to the fullest extent possible consistent with their countries' laws, any request for disclosure. Where the Participant that receives an application for disclosure from a third party is unable to obtain consent for its disclosure from the Requested Participant, if the Receiving Participant is nevertheless obliged under its laws to release the information, it should notify the Requested Participant as soon as possible of its decision to disclose the information, as well as the general procedure concerning the disclosure of information.

E. The Participants recognize that material exchanged in connection with investigations and enforcement often contains personally identifiable information. If the Requesting Participant wishes to obtain confidential information that includes personally identifiable information, then the Participants understand that they are to take additional appropriate measures to safely transmit and safeguard the materials containing personally identifiable information. Protective measures include, but are not limited to, the following examples and their reasonable equivalents, which can be used separately or combined as appropriate to particular circumstances:

1. transmitting the material in an encrypted format;

2. transmitting the material directly by a courier with package tracking capabilities;

3. transmitting the materials by facsimile rather than non-encrypted email;

4. maintaining the materials in secure, limited access locations (e.g., password-protected files for electronic information and locked storage for hard-copy information); and

5. if used in a proceeding that may lead to public disclosure, redacting personally identifiable information or filing under seal.

VI. **Changes in Applicable Privacy Laws**

In the event of significant modification to the Applicable Privacy Laws of a Participant's country falling within the scope of this Memorandum, the Participants intend to consult promptly, and, if possible, prior to the entry into force of such enactments, to determine whether to modify this Memorandum.

VII. **Retention of Information**

A. If Participants wish to retain materials obtained from the other Participant under this Memorandum, the Participants understand they are not to retain such materials for longer than is reasonably required to fulfill the purpose for which they were shared or for longer than is required by the Requesting Participant's country's laws.

B. The Participants recognize that in order to fulfill the purpose for which the materials were shared, the Participants typically need to retain the shared materials until the conclusion of the pertinent investigation or related proceedings for which the materials were requested, including until a judgment has become irrevocable.

C. The Participants are to use best efforts to return any materials that are no longer required if, at the time they are shared, the Requested Participant makes a written request that such materials be returned. If no request for return of the materials is made, then the Requesting Participant may dispose of the materials using methods prescribed by the Requested Participant, or if no such methods have been prescribed, by other secure methods, as soon as practicable after the materials are no longer required.

VIII. **Costs**

Unless otherwise decided by the Participants, the Requested Participant is expected to pay all costs of executing the request for information. When such costs are substantial, the Requested Participant may ask the Requesting Participant to pay those costs as a condition of proceeding with the Request. In such an event, the Participants should consult on the issue at the request of either Participant.

IX. **Duration of Cooperation**

A. The Participants intend cooperation in accordance with this Memorandum to become available as of the date it is signed by both Participants.

B. Assistance in accordance with this Memorandum is understood to be available concerning Covered Privacy Violations occurring before as well as after this arrangement is signed.

C. A Participant should endeavor to provide 30 days advance written notice to the other Participant that it plans to withdraw from the understanding set out in this Memorandum. However, prior to providing such notice, each Participant should use best efforts to consult with the other Participant.

D. Upon cessation of cooperation through this Memorandum, the Participants, in accordance with Section V, are to maintain the confidentiality of any information communicated to them by the other Participant in accordance with this Memorandum, and return or destroy, in accordance with the provisions of Section VII, information obtained from the other Participant in accordance with this Memorandum.

X. **Legal Effect**

Nothing in this Memorandum is intended to:

A. Create binding obligations, or affect existing obligations, under international or domestic law.

B. Prevent a Participant from seeking assistance from or providing assistance to the other Participant pursuant to other agreements, arrangements, or practices.

C. Affect any right of a Participant to seek information on a lawful basis from a Person located in the territory of the other Participant's country, or preclude any such Person from voluntarily providing legally obtained information to a Participant.

D. Create a commitment that conflicts with either Participant’s national laws, court orders, or any applicable international legal instruments.

E. Create expectations of cooperation that would exceed a Participant's powers.

Signed at Washington, D.C.
On March 6, 2015, in duplicate.

_____	_____
Edith Ramirez Chairwoman	Jacob Kohnstamm Chairman
United States Federal Trade Commission	Dutch Data Protection Authority

PROTOCOLE D'ENTENTE

ENTRE

LA COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA ET L' INFORMATION COMMISSONER DU ROYAUME-UNI

SUR

L'ENTRAIDE DANS LE CADRE DE L'APPLICATION DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ

La commissaire à la protection de la vie privée du Canada (la commissaire) et le Information Commissioner du Royaume-Uni (le « IC ») (« les participants ») :

RECONNAISSANT la nature de l'économie mondiale moderne, la circulation et la communication accrues des renseignements personnels d'un pays à l'autre, la complexité et le caractère envahissant des technologies de l'information et le besoin connexe de renforcer la coopération en matière d'application transfrontalière des lois;

RECONNAISSANT que la Recommandation de l'OCDE fixant un cadre pour la coopération dans l'application transfrontalière des lois sur la vie privée et le cadre de protection de la vie privée de l'APEC exhortent les pays et les économies membres à élaborer des mécanismes de communication des renseignements transfrontaliers et des ententes de coopération bilatérales ou multilatérales en matière d'application des lois;

RECONNAISSANT que l'article 23.1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5, autorise la commissaire à communiquer des renseignements à des autorités responsables de la protection des renseignements personnels dans le secteur privé d'autres pays;

RECONNAISSANT que le IC est l'autorité désignée au Royaume-Uni pour les fins de l'article 13 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature à Strasbourg, le 28 janvier 1981, et est l'autorité de contrôle au Royaume-Uni pour les fins de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données;

RECONNAISSANT que les participants ont chacun des attributions semblables en matière de protection des renseignements personnels dans le secteur privé dans leurs pays respectifs; et RECONNAISSANT que rien dans ce protocole n'exige aux participants à offrir quelconque assistance en matière d'application des lois de protection des renseignements personnels dans le secteur privé si une telle assistance serait interdit par leur lois domestiques ou politiques d'application respectives.

SE SONT ENTENDUS SUR CE QUI SUIT :

I. **Définitions**

Dans le cadre du présent protocole,

A. « lois applicables sur la protection des renseignements personnels » Lois et règlements du pays participant dont l'application permet de protéger les renseignements personnels. Dans le cas de la commissaire, la « loi applicable sur la protection des renseignements personnels » est la partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5 (LPRPDE) et, dans le cas du IC, la Data Protection Act 1998; ainsi que toute modification apportée aux lois applicables sur la protection des renseignements personnels des participants et d'autres lois et règlements que les participants peuvent décider conjointement, au fil du temps et par écrit, d'inclure dans la catégorie des lois applicables sur la protection des renseignements personnels du présent protocole d'entente.

B. « personne » Personne physique ou morale, y compris les sociétés par actions, les associations sans personnalité morale et les sociétés de personnes.

C. « demande » Demande d'aide aux termes du présent protocole d'entente.

D. « participant répondant » Participant à qui une aide est demandée aux termes du présent protocole d'entente ou qui fournit une telle aide.

E. « participant demandant » Participant qui demande l'aide aux termes du présent protocole d'entente ou qui la reçoit.

F. « contravention visée en matière de protection des renseignements personnels » Tout comportement qui contreviendrait aux lois applicables sur la protection des renseignements personnels du pays de l'un des participants qui est identique ou essentiellement semblable à un comportement qui constitue une contravention aux lois applicables sur la protection des renseignements personnels du pays de l'autre participant.

II. **Objectifs et portée**

A. Les participants reconnaissent qu'il est dans leur intérêt commun de faire ce qui suit :

1. coopérer dans le cadre du contrôle de l'application des lois applicables sur la protection des renseignements personnels, y compris en communiquant des renseignements pertinents et dans le cadre de l'instruction des plaintes dans lesquelles ils ont un intérêt mutuel;
2. faciliter les activités de recherche et de sensibilisation concernant la protection des renseignements personnels;
3. promouvoir une meilleure compréhension des conditions et des théories économiques et juridiques relatives à l'application des lois applicables sur la protection des renseignements personnels; et
4. se tenir informés des nouveaux événements dans leurs pays respectifs qui ont des répercussions sur le présent protocole d'entente.

B. Pour servir ces intérêts communs et conformément à la section IV, les participants feront de leur mieux pour réaliser ce qui suit :

1. communiquer des renseignements qui, selon eux, pourraient être utiles à une enquête ou à une poursuite en cours ou éventuelle relative à une contravention visée en matière de protection des renseignements personnels par les lois applicables sur la protection des renseignements personnels du pays de l'autre participant;
2. échanger et fournir des renseignements liés à des affaires visées par le protocole d'entente, comme des renseignements utiles pour la sensibilisation des consommateurs et des entreprises, des solutions en matière d'application de la loi issues du gouvernement ou de l'autoréglementation, des modifications aux textes législatifs connexes et des problèmes relatifs à la dotation et aux ressources; et

3. organiser des échanges de personnel à court terme et, éventuellement, à long terme, pour favoriser et renforcer la collaboration des participants dans le cadre d'activités d'application.

C. Pour servir ces intérêts communs et conformément à la section IV, les participants reconnaissent que l'élément suivant est un enjeu prioritaire exigeant une éventuelle coopération :

1. éventuelle enquête ou mesure d'application parallèle ou conjointe des participants.

III. Procédures d'entraide

A. Chaque participant nommera une personne-ressource principale qui traitera les demandes d'aide et les autres communications entre les parties du protocole d'entente.

B. Lorsqu'ils demandent de l'aide relativement à des procédures ou à des enquêtes ou pour d'autres motifs touchant l'application transfrontalière des lois applicables sur la protection des renseignements personnels, les participants s'assureront que :
   1. les demandes d'aide contiennent suffisamment de renseignements pour que le participant répondant puisse déterminer si elles sont liées à une contravention visées en matière de protection des renseignements personnels et s'il doit intervenir dans les circonstances appropriées. De tels renseignements peuvent inclure une description des faits sous-jacents à la demande et le type d'aide demandée ainsi qu'une indication de toute précaution spéciale à prendre pour donner suite à la demande;
   2. les demandes d'aide précisent à quelle fin les renseignements demandés seront utilisés; et
   3. avant de demander de l'aide, les participants réalisent une enquête préliminaire pour confirmer que la demande est conforme à la portée du présent protocole d'entente et ne constitue pas un fardeau excessif pour le participant répondant.

C. Les participants prévoient communiquer et collaborer entre eux, s'il y a lieu, quand cela peut contribuer aux enquêtes en cours.

D. Les participants informeront les autres sans délai s'ils constatent que certains renseignements communiqués dans le cadre du présent protocole d'entente sont inexacts, incomplets ou périmés.

E. Sous réserve de la section IV, les participants peuvent, si cela est approprié et conforme à leurs lois applicables sur la protection des renseignements personnels, se renvoyer des plaintes ou s'informer de possibles contraventions visées en matière de protection des renseignements personnels par les lois applicables sur la protection des renseignements personnels du pays de l'autre participant.

F. Les participants feront de leur mieux pour régler tout désaccord concernant la coopération dans le cadre du présent protocole d'entente par le truchement des personnes-ressources désignées à la section III (A). Si celles-ci sont incapables de régler le problème après un délai raisonnable, les responsables des participants en discuteront.

IV. Limites liées à l'aide et à l'utilisation

A. Le participant répondant peut exercer son pouvoir discrétionnaire et refuser de répondre à une demande d'aide, limiter sa coopération ou imposer des conditions connexes, particulièrement lorsque la demande n'est pas visée par le présent protocole d'entente ou, plus généralement, lorsque cela est contraire à ses lois ou à des intérêts et priorités importants. Le participant demandant peut demander les motifs pour lesquels le participant répondant a refusé de l'aider ou a limité son aide.

B. Les participants communiqueront uniquement des renseignements personnels dans le cadre du présent protocole d'entente dans la mesure où cela est nécessaire à la réalisation des objectifs du protocole. En outre, quand cela est

possible, ils feront de leur mieux pour obtenir au préalable le consentement des personnes concernées.

C. Pour plus de certitude, la commissaire ne communiquera pas de renseignements confidentiels sauf :

   a. aux fins établies à la section II (B.1);
   b. s'il est nécessaire de le faire pour présenter une demande d'aide à l'autre participant concernant les renseignements pouvant être utiles dans le cadre d'une enquête ou d'une vérification en cours ou éventuelle aux termes de la partie 1 de la LPRPDE.
   Les participants n'utiliseront pas les renseignements fournis par le participant répondant à d'autres fins que celles auxquelles ils ont été communiqués.

Confidentialité

Les renseignements communiqués dans le cadre du présent protocole d'entente seront traités de manière confidentielle et ne seront pas autrement communiqués sans le consentement de l'autre participant.

Chaque participant fera de son mieux pour protéger les renseignements fournis aux termes du présent protocole d'entente et respecter toutes les mesures de protection établies par les participants. En cas de consultation ou de communication non autorisée des renseignements, les participants mettront en place toutes les mesures nécessaires pour empêcher que cela se reproduise et informeront rapidement l'autre participant de la situation.

Les participants feront tout en leur pouvoir, dans les limites des lois de leur pays, pour s'opposer à toute demande par une tierce partie de communication de renseignements ou de documents confidentiels fournis par le participant répondant, sauf si celui-ci consent à la communication. Les participants qui recevront une telle demande en informeront rapidement le participant qui a fourni les renseignements confidentiels.

Modification des lois applicables sur la protection des renseignements personnels

En cas de modification des lois applicables sur la protection des renseignements personnels du pays d'un participant qui sont visées par le présent protocole d'entente, les participants feront de leur mieux pour se consulter rapidement et, si possible, avant l'entrée en vigueur desdites modifications, pour déterminer s'il faut modifier le présent protocole d'entente.

Conservation des renseignements

Les renseignements reçus dans le cadre du présent protocole d'entente ne seront pas conservés plus longtemps que nécessaire pour la réalisation de l'objectif à l'origine de la communication ou plus longtemps que l'exigent les lois du pays du participant demandant. Les participants feront de leur mieux pour renvoyer tous les renseignements qui ne sont plus requis si le participant répondant a demandé par écrit le renvoi des renseignements au moment de la communication. Si le participant répondant ne demande pas le renvoi des renseignements, le participant demandant en disposera à l'aide des méthodes définies par le participant répondant ou, si ce dernier n'a pas précisé les méthodes, grâce à des méthodes sécuritaires, le plus rapidement possible une fois que les renseignements ne seront plus nécessaires.

Coûts

Sauf si les participants en décident autrement, le participant répondant engagera tous les coûts nécessaires pour répondre à la demande. Lorsque les coûts liés à la communication ou l'obtention de renseignements dans le cadre du présent protocole d'entente sont importants, le participant répondant peut demander au participant demandant de les payer en tant que condition au traitement de la demande. Dans une telle situation, les participants procéderont à des consultations sur la question à la demande d'un des participants.

Durée de la coopération

Le présent protocole d'entente entre en vigueur à la date de signature.
L'aide prévue dans le présent protocole d'entente sera fournie relativement à des contraventions visées qui se sont produites avant et après la signature du protocole d'entente.
Les participants peuvent mettre fin au présent protocole d'entente en envoyant un avis écrit de 30 jours à l'autre participant. Cependant, avant de donner un tel avis, chaque participant fera de son mieux pour consulter l'autre participant.
Ce protocole peut être modifié, ou complété, tel que convenu par les participants par écrit.
Lorsque le protocole d'entente ne sera plus en vigueur, les participants continueront à assurer la confidentialité des renseignements communiqués par l'autre participant dans le cadre du présent protocole d'entente conformément à la section V, et renverront ou détruiront les renseignements fournis par l'autre participant dans le cadre du présent protocole d'entente conformément aux dispositions de la section VII.

Conséquences juridiques

Aucune disposition du présent protocole d'entente ne vise :

à créer des obligations contraignantes ou à influer sur des obligations existantes aux termes du droit international, ou à créer des obligations aux termes des lois des pays des participants;
à empêcher un participant de demander l'aide de l'autre participant ou de lui en fournir dans le cadre d'autres ententes, traités, arrangements ou pratiques;
à avoir un impact sur le droit d'un participant à tenter d'obtenir des renseignements de façon légale d'une personne située dans le pays de l'autre participant ni à empêcher une telle personne de fournir volontairement des renseignements obtenus légalement à un participant; ou
à créer des obligations ou des attentes de coopération qui dépassent la compétence des participants.

Signé le 14 mai 2012 à Montréal, Québec, Canada en deux exemplaires, en français et en anglais, toutes les versions étant également valides.

La version originale est signée par

Christopher Graham
Information Commissioner du Royaume-Uni

Date: 2012-05-14
À: Montréal, Québec, Canada

La version originale est signée par

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Date: 2012-05-14
À: Montréal, Québec, Canada

ANNEXE C

Lettre aux opérateurs du site diffusant des images de caméras Web

Le 21 novembre 2014

Mesdames,
Messieurs,

Nous vous écrivons en tant qu'autorités chargées de l'application des lois sur la protection des renseignements personnels pour faire le point sur un important problème qui a été porté à notre attention.

Nous avons de sérieuses préoccupations concernant votre site Web et les séquences vidéo que vous diffusez en direct à partir de caméras Web dont les propriétaires ont conservé le nom d'utilisateur et le mot de passe par défaut fournis par le fabricant. Ces caméras se trouvent dans des lieux privés ou des espaces publics et commerciaux, y compris des lieux de travail, et ce partout dans le monde.

Sur votre site Web, il est indiqué que cette pratique vise à démontrer l'importance de régler les paramètres de sécurité des caméras de surveillance. Nous reconnaissons en principe l'importance de mettre en lumière les problèmes potentiels liés à la sécurité, mais nous estimons que cela devrait se faire d'une façon qui ne porte pas atteinte aux gens.

Compte tenu de la nature délicate des renseignements personnels recueillis au moyen de ces caméras, particulièrement celles se trouvant dans les maisons, et du fait que votre site Web communique ces renseignements personnels sans que les individus filmés en soient conscients, cela constitue une grave menace pour la vie privée des gens du monde entier. Cette menace est accentuée par l'inclusion d'information sur l'emplacement géographique précis des caméras.

De plus, comme vous le savez sans doute, cette question a beaucoup retenu l'attention des médias. L'intérêt accru du public entraînera un risque encore plus important que les caméras accessibles à distance portent atteinte à la vie privée des personnes.

Par conséquent, nous vous demandons de prendre des mesures immédiates afin de fermer ce site Web. Nous vous demandons en outre d'éviter de recréer ce site à l'avenir, que ce soit sous son nom actuel ou tout autre nom, s'il continue de diffuser toute séquence vidéo montrant des individus et que ces derniers ne savent pas que la séquence vidéo en question fait l'objet d'une communication. Si vous ne vous conformez pas à cette demande d'ici au 26 novembre 2014 (00:00 UTC), nous envisagerons de prendre des mesures supplémentaires d'application de la loi.

Veuillez agréer, Mesdames, Messieurs, nos salutations distinguées.

Le commissaire à la protection de la vie privée de l'Australie,

Original signé par

Timothy Pilgrim

Le commissaire à la protection de la vie privée du Canada,

Original signé par

Daniel Therrien

La coordonnatrice, Office for Personal Data Protection of Macao – Chine,

Original signé par

Chan Hoi Fan

Le commissaire adjoint à l'information du Royaume-Uni,

Original signé par

David Smith

Le président de la Commission d'accès à l'information du Québec,

Original signé par

M^{e} Jean Chartier

La commissaire à l'information et à la protection de la vie privée de l'Alberta,

Original signé par

Jill Clayton

La commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique,

Original signé par

Elizabeth Denham

Les autorités chargées de la protection des données exhortent Google à donner suite aux préoccupations concernant Google Glass

Ottawa, le 18 juin 2013

Monsieur Larry Page
Chef de la direction
Google Inc.
1600 Amphitheatre Parkway
Mountain View, California
USA 94043

Monsieur,

Nous vous écrivons à titre d'autorités de protection des données personnelles afin de soulever, du point de vue du droit à la vie privée, des questions entourant le développement de Google Glass, un type d'ordinateur vêtement sous forme de lunettes[1], présentement en phase de test bêta et n'étant pas encore disponible au grand public.

Vous avez constaté bien entendu que Google Glass a fait l'objet de nombre d'articles qui soulèvent des préoccupations au sujet des répercussions évidentes, et peut-être moins évidentes, sur le plan de la vie privée découlant d'un appareil qui peut être porté par une personne et qui peut servir à produire des enregistrements audio et vidéo d'autres personnes. Des craintes ont été soulevées quant à la surveillance ubiquiste d'individus par d'autres individus, que ce soit par l'entremise de tels enregistrements ou d'autres applications présentement en développement. Des questions quant à la collecte de telles données par Google et quant à leur utilisation se posent également au regard de la nouvelle politique de confidentialité de Google.

Comme vous le savez sans doute, les autorités de protection des données insistent depuis longtemps sur la nécessité pour les organisations de tenir compte des principes de protection des données personnelles dès l'étape de la conception des produits et services, avant le lancement de ceux-ci. En outre, plusieurs d'entre nous enjoignons les organisations à consulter de manière significative nos autorités respectives.

À ce jour, tout ce que nous savons au sujet de Google Glass, de son mode d'opération, de ses usages potentiels et de l'utilisation que Google pourrait faire des données recueillies par l'entremise de Glass provient en grande partie d'articles de presse, largement fondés sur des hypothèses, et de la publicité effectuée par Google elle-même au sujet de l'appareil.

Par exemple, nous avons cru comprendre que pendant la phase de test bêta du produit, Google a mis en place des lignes directrices détaillées à l'intention des développeurs d'applications qui conçoivent des programmes destinés à Glass[2]. Les limites qui leur sont imposées semblent porter en grande partie sur la publicité à l'intérieur de Glass. Si c'est effectivement le cas, nous y verrions une première étape positive dans le repérage des enjeux de vie privée, mais il ne s'agirait que d'une première étape et de la seule dont nous serions au courant.

Nous savons que d'autres entreprises développent également des produits semblables, mais la vôtre est un chef de file en la matière, la première à faire l'essai d'un produit in situ, et la première à envisager les enjeux éthiques soulevés par un tel produit. Jusqu'à présent, toutefois, votre entreprise n'a toujours pas communiqué avec la majorité des autorités de protection des données personnelles signataires de la présente pour discuter de l'un ou l'autre des enjeux en cause.

Pour notre part, nous exhortons Google à entamer un dialogue significatif avec les autorités de protection des données au sujet de Glass.

Nous voudrions soulever entre autres les questions suivantes :

- Comment Google Glass se conforme-t-il aux lois sur la protection des données?
- Quelles mesures de protection des données personnelles Google et les développeurs d'application mettent-ils en place?
- Quels renseignements Google recueille-t-elle par l'entremise de Glass et quels renseignements sont transmis à des tiers, y compris des développeurs d'applications?
- Comment Google compte-t-elle utiliser cette information?
- Bien que nous croyions comprendre que Google a choisi de ne pas intégrer la reconnaissance faciale à Glass, comment Google prévoit-elle aborder les enjeux liés à la reconnaissance faciale à l'avenir?
- Google fait-elle quoi que ce soit au sujet des grands enjeux sociétaux et éthiques soulevés par un tel produit, en outre, au sujet de la collecte subreptice d'information au sujet d'autres individus?
- Google a-t-elle déjà entrepris des évaluations des risques à la vie privée dont elle serait disposée à partager les conclusions avec nous?
- Google serait-elle disposée à faire une démonstration de l'appareil à l'intention de nos organisations, et de permettre à toute autorité de protection des données qui en fait la demande de soumettre l'appareil à des tests?

Nous sommes conscients que ces questions portent sur des enjeux qui sont de notre ressort en tant qu'autorité de protection des données, de même que sur des enjeux éthiques plus vastes soulevés par les ordinateurs vêtements. Nous serions très intéressés à en savoir davantage au sujet de l'incidence sur la vie privée de ce nouveau produit, et des mesures que vous envisagez adopter afin de vous assurer que le droit à la vie privée des personnes est respecté partout dans le monde, alors que vous allez de l'avant avec Google Glass. Nous attendons de vos nouvelles à ce sujet et nous espérons avoir l'occasion de prendre part à une rencontre afin de discuter des enjeux de vie privée soulevés par Google Glass.

Veuillez agréer, Monsieur, l'expression de nos sentiments distingués,

La commissaire à la protection de la vie privée du Canada,

Original signé par

Jennifer Stoddart

Le président du Groupe de travail de l'Article 29, au nom des membres du Groupe de travail de l'Article 29,

Original signé par

Jacob Kohnstamm

Le commissaire à la vie privée de l'Australie,

Original signé par

Timothy Pilgrim

La commissaire de la protection de la vie privée de la Nouvelle-Zélande,

Original signé par

Marie Shroff

Le secrétaire à la protection des données de l'Institut fédéral de l'Accès à l'information et la Protection des données du Mexique,

Original signé par

Alfonso Oñate Laborde

Le chef de la Israeli Law, Information and Technology Authority (Israël),

Original signé par

Rivki Dvash

Le préposé fédéral à la protection des données et à la transparence (Suisse),

Original signé par

Hanspeter Thür

La commissaire à la protection de la vie privée de l'Alberta,

Original signé par

Jill Clayton

Le président de la Commission d'accès à l'information du Québec,

Original signé par

Jean Chartier

La commissaire à la protection de la vie privée de la Colombie-Britannique,

Original signé par

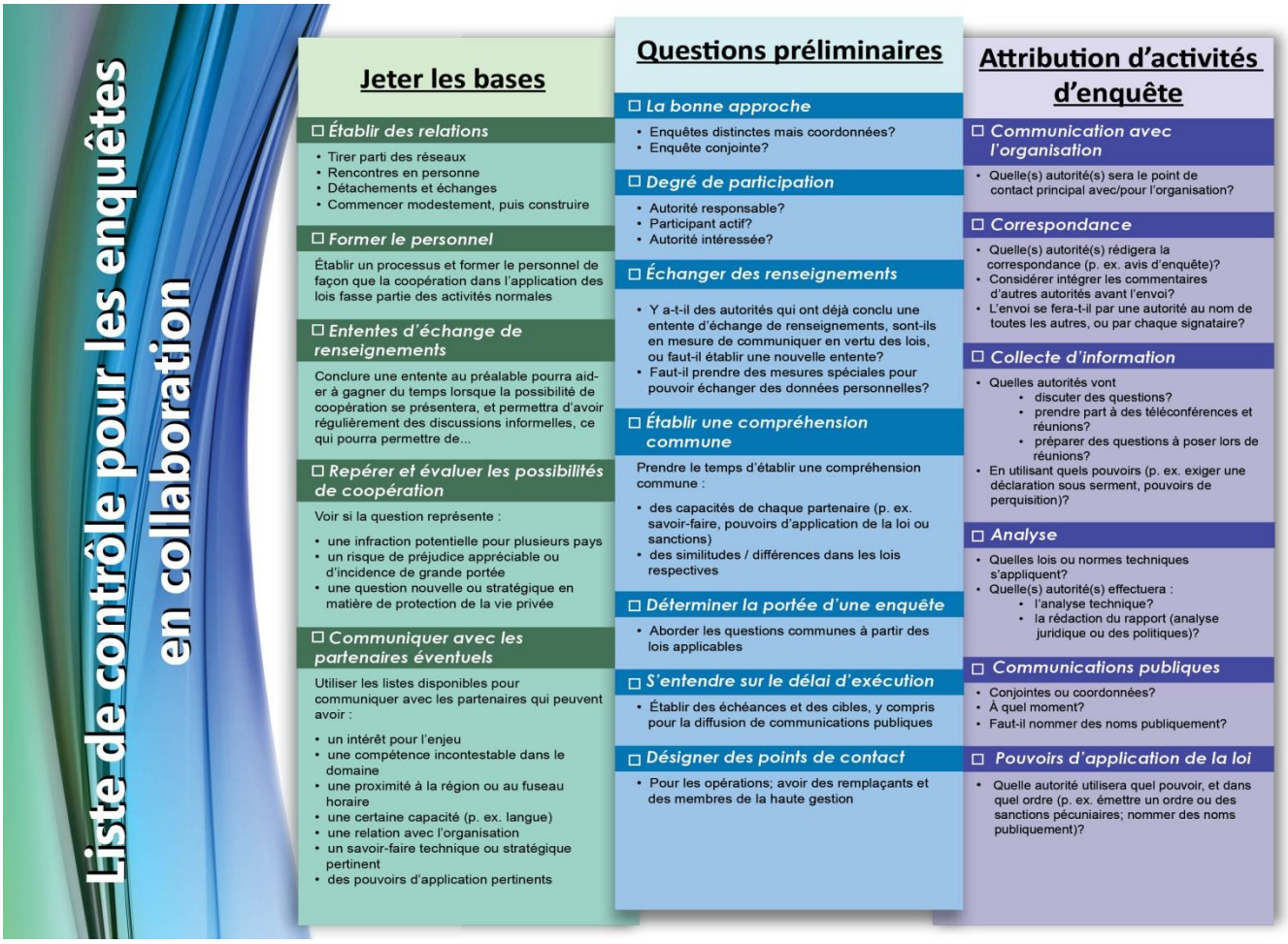
Elizabeth Denham

[1] Google Glass comprend une caméra, un micro et un GPS, avec connectivité Internet. Google Glass fonctionne à partir du système d'exploitation Android, et des tierces parties développent présentement des applications pour Glass. Pour accéder à Glass, l'utilisateur doit disposer d'un compte Google.

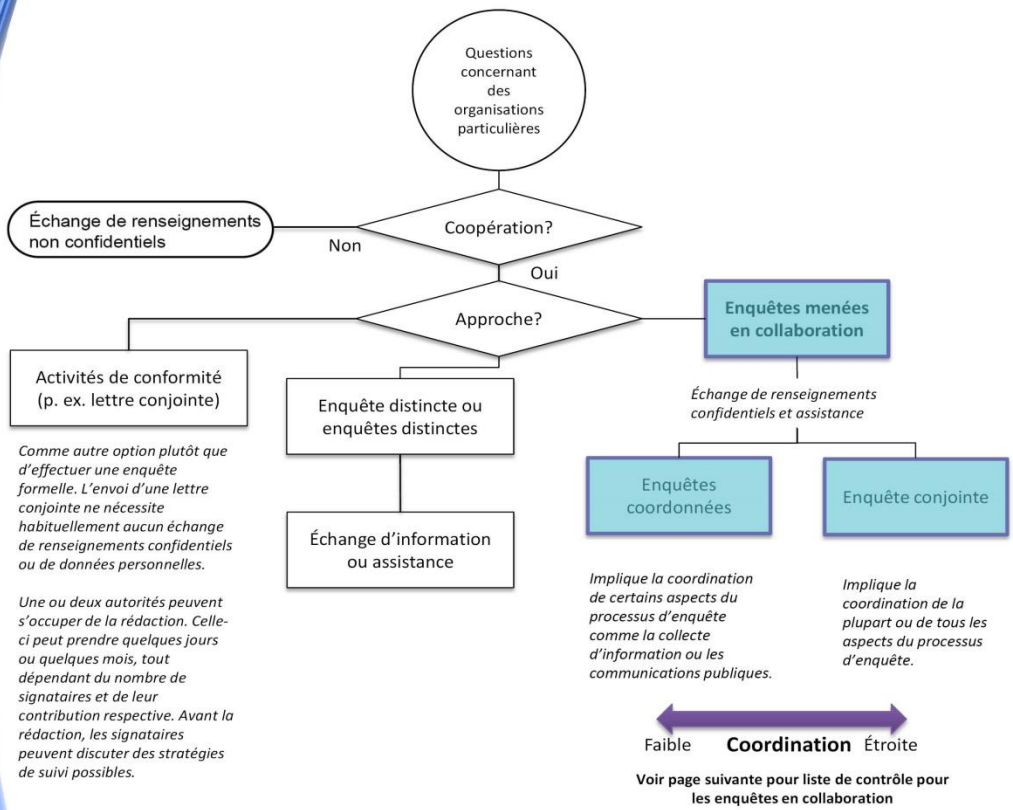
[2] https://developers.google.com/glass/overview

ANNEXE D

Aide-mémoire sur la coopération dans l'application des lois



Graphique de cheminement de la coopération dans l'application des lois



Voir page suivante pour liste de contrôle pour les enquêtes en collaboration

ANNEXE E

Exemple de modèle – protocole sur la coopération dans l'application transfrontière des lois

Liste de contrôle pour la coopération dans l'application des lois

Étape d'exploration

1. Organisation (nom et adresse, le cas échéant)

2. **Enjeu**

• Brève description de l'enjeu • Élément ayant permis de cerner l'enjeu (p. ex. plainte, médias ou autre autorité de protection des données personnelles) • Aspects internationaux

3. **L'enjeu relève-t-il de votre compétence?** Oui Non À déterminer

4. **Partenaires éventuels dans l'application de la loi**

Autorité	Base de coopération possible
Nom et territoire	• Organisation exerçant ses activités sur le territoire de l'autorité • Intérêt exprimé par l'autorité

5. **Votre autorité a-t-elle le pouvoir d'échanger des renseignements personnels dans ce dossier?**
Oui Non

Capacité d'échanger de l'information	• Fondements juridiques, restrictions (dans la négative, discussions de haut niveau uniquement)

6. **Premier contact avec l'autorité**

Autorisation (antérieure) donnée par :	• P. ex. directeur
Coordonnées	Nom, titre et coordonnées

Structure	**Information recherchée**
Intérêt ou enquête?	Oui ou non
Raison de l'intérêt pour l'enjeu	• Plaintes reçues • Enquête en cours ou nécessité de faire enquête • Enjeu grave ayant une incidence sur les individus
Intérêt pour la coopération ou l'échange d'information	Oui ou non

Partage des connaissances (lorsque la loi l'autorise)	• Résumé de la compréhension de l'autorité, des éléments de preuve déjà recueillis et des différences importantes par rapport à sa propre compréhension
Examen des bénéfices potentiels de la coopération ou de l'échange d'information	• Compétence et lien avec l'organisation • Proximité et langue • Capacité ou pouvoir d'accéder aux éléments de preuve pertinents • Savoir-faire particulier (stratégique ou technique)

7. Recommandations de l'enquêteur

- i) Aucune mesure requise de la part de votre autorité
- ii) Enquête menée par votre autorité ou par une autre autorité agissante seule, avec échange d'information
- iii) Enquête coordonnée par votre autorité ou par une autre autorité (certains aspects de l'enquête peuvent être coordonnés – voir 10b] ci-après)
- Justification : autre autorité intéressée; avantages et possibilités pour votre autorité

Étape d'enquête

8. Approbation de l'approche de coopération (cadre supérieur)

9. Compréhension et approbation des modalités de l'échange d'information

Organisations échangeant l'information	• Votre autorité, autre autorité ou les deux
Type d'information à échanger	• P. ex. mises à jour sur l'enquête et éléments de preuve
Fréquence	• P. ex. à la réception ou mensuellement
Restrictions et exigences	• Fondements juridiques, mesures de protection, traitement des données personnelles ou restrictions relatives à la publication

10. Enquête menée en collaboration

a. Questions préliminaires

Votre autorité mènera-t-elle l'enquête ou enquêtera-t-elle en collaboration?	• Volonté ou besoin des deux autorités de faire enquête • Possibilité de regrouper les ressources pour accroître l'efficience ou l'incidence
Compréhension de la législation régissant le partenaire	• Similitudes et différences importantes • Pouvoirs d'application des lois et pouvoirs de collecte des éléments de preuve • Restrictions relatives à la communication au public
Établissement de la portée de l'enquête	• Enjeux visés par l'enquête (y compris les différences entre les autorités)
Délai d'exécution ou jalons convenus	• Avis à l'organisation • Communication de mise à jour périodique • Achèvement de l'enquête et publication des conclusions

Contacts	Contact pour l'enquête
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)
	Contact suppléant pour l'enquête
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)
	Contact de la direction
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées
	Autre (p. ex. technologie)
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)

b. Coordination des activités d'enquête et d'application des lois

Point de contact au sein de l'organisation	• Un contact au sein de chaque autorité
Correspondance avec l'organisation	• Correspondance conjointe ou distincte (mais généralement coordonnée)
Collecte d'information auprès de l'organisation	• Qui recueillera quelle information et en vertu de quelle autorité (généralement de façon coordonnée)?
Analyse des éléments de preuve	• P. ex. analyse technique ou juridique
Communications publiques	• Communications conjointes ou coordonnées (envoi de messages ou moment des communications)
Atteinte de la conformité ou application de la loi	• Quels pouvoirs seront utilisés et qui les utilisera (désignation, pénalités ou conformité obligatoire)?

11. Approbation de l'approche finale (p. ex. cadre supérieur ou directeur chargé de l'application des lois)

(Il faut généralement obtenir une approbation pour apporter toute modification importante au présent modèle.)

Glossaire

Le présent glossaire a pour objet d'expliquer aux rédacteurs la signification de certains termes utilisés dans le guide. Il prend acte du fait que les autorités peuvent donner des définitions différentes mais tout aussi valables de ces termes conformément à leur cadre juridique. Les explications ne sont donc pas données dans le but d'obtenir, voire de suggérer leur acceptation générale. Le glossaire doit uniquement être utilisé pour interpréter et comprendre le présent guide. Les autorités de chaque pays sont les mieux placées pour évaluer dans quelle mesure cela concorde avec la terminologie locale.

1. **entente (ou protocole d'entente) :** Document n'ayant pas force exécutoire signé par plusieurs autorités d'exécution des lois sur la protection de la vie privée, qui précise l'accord intervenu entre les signataires, les situations et les conditions en vertu desquelles ces autorités peuvent coopérer dans le cadre d'activités d'application de la loi et, en particulier, échanger des renseignements confidentiels ou des données personnelles. Rien dans ce type de document n'exige que les signataires se prêtent main-forte dans l'application des lois si cette assistance est interdite par des lois nationales ou applicables ou par les politiques en matière d'application de la loi. Aux fins du présent guide, nous n'établissons pas de distinction entre une entente et un protocole d'entente.

2. **coopération :** Regroupement de plusieurs autorités pour favoriser l'application de mesures de protection de la vie privée, ayant les objectifs suivants : i) la communication d'une politique non confidentielle ou d'information pratique; ii) l'échange de renseignements confidentiels ou de données personnelles ; ou iii) la coordination des activités aux fins d'activités en matière d'application de la loi ou de conformité dans un autre domaine.

    a. **coordination :** Forme de coopération dans le cadre de laquelle plusieurs autorités établissent des liens entre leurs activités (ou les coordonnent) en relation avec des activités particulières d'application des lois (p. ex. enquête menée en collaboration ou initiative en matière de conformité dans un autre domaine – p. ex. lettre conjointe ou ratissage).

        i. **enquête menée en collaboration :** Une forme de coordination dans le cadre de laquelle plusieurs autorités coordonnent leurs activités en relation avec des activités d'application des lois connexes dans leurs pays respectifs (p. ex. collecte de renseignements, analyse technique, communication publique de résultats). L'enquête requiert généralement la communication de renseignements confidentiels ou de données personnelles. Le niveau de collaboration (p. ex. le nombre d'activités que les autorités choisissent de coordonner) peut être restreint ou vaste.

3. **renseignements confidentiels** : Renseignements qu'une « autorité qui communique » fournit à une « autorité qui reçoit » (ensemble, « les autorités coopérantes »), étant entendu que, sous réserve de toute autre entente entre les autorités coopérantes, l'autorité qui reçoit s'assurera que les renseignements ne sont accessibles qu'aux personnes relevant de sa compétence et devant avoir accès à ces renseignements aux fins où ils ont été communiqués (p. ex. en relation avec une enquête précisée). Les renseignements confidentiels sont souvent des renseignements

se rapportant à une activité en matière d'application de la loi en cours ou éventuelle qui peut inclure ou non des données personnelles. Ils peuvent également comporter d'autres types de renseignements stratégiques non publics ou ayant trait à la politique.

4. **données personnelles (ou renseignements personnels) :** Information sur une personne qui est, dans de nombreux pays, visée par des exigences particulières en vertu des lois sur la protection de la vie privée ou des renseignements (p. ex. comme il est précisé à l'article 7 et à l'annexe I de l'Entente). Les données personnelles seront, dans la plupart des cas, des renseignements confidentiels. Pour les besoins exclusifs du présent guide, nous n'établirons pas de distinction entre les « données personnelles » et les « renseignements personnels ».

5. **activité en matière d'application de la loi ou activité en matière de conformité :**

   a. **activité en matière d'application de la loi :** mesure(s) prise(s) par une autorité d'exécution des lois sur la protection de la vie privée dans le but soit : i) d'exiger qu'une organisation (ou un particulier) se conforme à la législation sur la vie privée ; ou ii) de pénaliser l'organisation ou le particulier en question qui ne se conforme pas.

   b. **activité en matière de conformité :** mesure(s) prise(s) par une autorité d'exécution des lois sur la protection de la vie privée dépassant le cadre de ses pouvoirs d'exécution pour encourager la conformité volontaire des organisations ou des particuliers aux lois sur la protection de la vie privée ou à des pratiques exemplaires.

6. **Compétence (juridiction) :** Portée (prévue par la loi) des responsabilités d'une autorité d'exécution des lois pour la protection de la vie privée;

7. **Pays :** Région géographique ou territoire où une autorité a la responsabilité d'appliquer la législation des lois sur la protection de la vie privée.

8. **Autorité d'exécution des lois sur la protection de la vie privée (ou « autorité ») :** Autorité ayant la responsabilité de promouvoir la conformité aux lois sur protection de la vie privée ou d'obliger à la conformité sur un territoire donné. Aux fins du présent guide, le terme inclut les autorités assurant la protection des données.