31ème Conférence des commissaires à la protection des données et à la vie privée

Madrid, Espagne
4-6 novembre 2009

Résolution sur des normes internationales de vie privée

Sponsors :

- Autorité de protection des données (Espagne)
- Autorité de protection des données (Suisse)
- Contrôleur européen de la protection des données
- Autorité de protection des données (France)
- Commissaire à la protection des données (Irlande)
- Autorité de protection des données (République Tchèque)
- Autorité de protection des données (Allemagne)
- Autorité de protection des données (Italie)
- Autorité de protection des données (Pays-Bas)
- Commissaire à la protection des données (Nouvelle-Zélande)
- Commissaire à la protection des données (Grande Bretagne)

Co-Sponsors :

- Autorité de protection des données (Andorre)
- Autorité de protection des données (Catalogne)
- Autorité de protection des données (Communauté de Madrid)
- Autorité de protection des données (Pays Basque)
- Autorité de protection des données (Ile de Man)
- Autorité de protection des données (Estonie)
- Autorité de protection des données (Lituanie)
- Autorité de protection des données (Berlin)
- Autorité de protection des données (Schleswig-Holstein)
- Autorité de protection des données (Argentine)
- Commissaire à la protection des données (Malte)
- Autorité de protection des données (Burkina Faso)
- Commissaire à la protection des données (Chypre)
- Autorité de protection des données (Finlande)
- Commissaire à la protection des données (Slovénie)
- Autorité de protection des données (Grèce)

Note que :

- la 30ème Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée a unanimement adopté à Strasbourg la **résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une Proposition Conjointe d'établissement de Normes Internationales sur la Vie Privée et la Protection des Données Personnelles.**

- La résolution donnait mandat pour créer un groupe de travail, coordonné par l'autorité espagnole de protection des données, organisateur de la 31è Conférence, et composé des autorités de protection des données intéressées, pour rédiger et soumettre à la 31ème Conférence une **Proposition Conjointe visant à établir des Normes Internationales sur la Vie Privée et la Protection des Données Personnelles.**

- Dans le cadre de ce mandat, l'autorité espagnole de protection des données a établi un groupe de travail, promu et coordonné le travail d'élaboration d'une Proposition Conjointe pour un projet de Normes Internationales.

- Le groupe de travail a rédigé une **Proposition Conjointe pour un Projet de Normes Internationales sur la Protection de la Vie Privée au regard du Traitement de Données Personnelles**, basée sur les principes présents dans les différents instruments, lignes directrices, recommandations de portée internationale et qui ont obtenu un large consensus dans leurs zones géographiques, économiques et juridiques respectives.

- La Proposition Conjointe a été rédigée en assumant que tous ces principes et approches communes apportent des éléments de valeur dans la défense et l'amélioration de la vie privée et des informations personnelles, dans le but de les étendre en ajoutant des solutions et des dispositions spécifiques qui pourraient s'appliquer indépendamment des différences qui pourraient exister entre les différents modèles existants de protection des données personnelles et de la vie privée.

Par conséquent, la Conférence décide :

1. D'accueillir la Proposition Conjointe pour un Projet de Normes Internationales de Protection de la Vie Privée au regard de la Protection des Données Personnelles annexée à cette résolution. La Proposition Conjointe démontre la faisabilité de telles normes, comme une nouvelle étape vers le développement en temps voulu d'un instrument international contraignant.

2. D'affirmer que la Proposition Conjointe fournit un ensemble de principes, droits, obligations et procédures que tout système juridique de protection des données personnelles et de la vie privée devrait s'efforcer de respecter. Dans cette perspective, le traitement de données personnelles dans les secteurs publics et privés serait effectués, avec une approche internationale plus uniforme :

    a. Loyalement, légalement et d'une manière appropriée en relation avec des finalités spécifiques, explicites et légitimes ;
    b. Sur la base de politiques transparentes, informant de façon adéquate les personnes concernées et sans discrimination arbitraire à leur encontre ;
    c. S'assurant de la justesse, de la confidentialité et de la sécurité des données, de la légitimité du traitement, ainsi que des droits des personnes concernées d'accéder, de rectifier, de supprimer leurs données et de leur droit de s'opposer au traitement ;
    d. Mettant en place des principes « d'accountability » et de responsabilité, et ce même si les opérations de traitement des données sont effectuées par des prestataires pour le compte du responsable de traitement ;
    e. Offrant des garanties plus appropriées lorsque les données sont sensibles ;
    f. S'assurant que les données personnelles transférées au niveau international bénéficient d'un niveau de protection prévu dans les normes ;
    g. Sujettes au contrôle d'autorités de supervision indépendantes et impartiales dotées de ressources et de pouvoirs adéquats et en lien avec leur devoir de coopération entre elles ;
    h. Dans un cadre nouveau et moderne de mesures proactives, comme celles visant en particulier à prévenir et détecter les failles et basées sur la désignation de correspondants à la protection des données, ainsi que sur des études d'impacts et des audits efficaces.

3. D'inviter les Autorités de Protection des Données et de la Vie Privée accréditées à la Conférence Internationale à circuler aussi largement que possible cette Proposition Conjointe pour un Projet de Normes Internationales sur la Vie Privée au regard du Traitement de Données Personnelles.

4. De confier aux autorités organisatrices de la 31ème et 32ème Conférence Internationale de coordonner le Groupe de Promotion, composé des autorités de protection des données intéressées, qui sera responsable de :
    a. Circuler et promouvoir la Proposition Conjointe parmi les entités privées, experts, autorités nationales et internationales pertinents comme une base pour de futurs

travaux vers le développement d'une convention internationale contraignante, et en particulier aux entités et organisations mentionnées dans la Déclaration de Montreux ; et

b. Explorer et rendre compte des autres possibilités d'utilisation de la Proposition Conjointe comme une base pour développer l'entente et la coopération internationale en matière de protection des données et de la vie privée, en particulier dans un contexte de permission de transferts internationaux de données personnelles qui auraient lieu de telle sorte que seraient sauvegardés les droits et libertés des individus.

5. De demander au Groupe de Promotion :
   a. De coordonner son travail avec le Comité de Direction de la Conférence chargé de la Représentation devant les Organisations Internationales, et
   b. De rendre compte de tout progrès lors de la 32ème Conférence Internationale pour assurer une attention continue sur cette résolution

Note explicative

La 30ème Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée a adopté une **Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et d'élaborer d'une Proposition Conjointe pour l'établissement de Normes Internationales sur la Vie Privée et la Protection des Données Personnelles**, proposée conjointement par les autorités suisse et espagnole de protection des données et soutenue par vingt autres autorités.

Dans cette résolution, la Conférence rappelait plusieurs déclarations et résolutions adoptées au cours des dix dernières années dont l'objectif était de renforcer le caractère universel du droit à la protection des données et de la vie privée, et qui appelaient au développement d'une convention universelle pour la protection des personnes au regard du traitement de leurs données personnelles.

De plus, la résolution annonçait que la Conférence considérait les droits à la protection des données et à la vie privée comme des droits fondamentaux des personnes, sans distinction de nationalité et de lieu de résidence, tout en constatant que les différences persistantes en termes de protection des données et de la vie privée au niveau mondial, dues notamment au fait que de nombreux pays n'ont pas encore adopté de loi adéquate, nuisent aux échanges de données personnelles et à la mise en œuvre efficace d'une protection des données au niveau mondial.

Par conséquent, la résolution exprimait la conviction de la Conférence que la reconnaissance de ces droits requiert l'adoption d'un instrument juridique mondial contraignant, lequel recensera et complètera les principes communs de protection des données recensés dans plusieurs instruments juridiques existants, et renforcera la coopération internationale entre les autorités de protection des données.

A cet égard, la résolution exprimait le soutien de la Conférence aux efforts du Conseil de l'Europe pour améliorer les droits fondamentaux à la protection des données et à la vie privée, et invite les États, membres ou non de l'organisation, à ratifier la Convention pour la protection des personnes à l'égard des traitements de données et son protocole additionnel, et réitère le soutien de la Conférence pour les actions menées par l'APEC, l'OCDE et les autres forums internationaux et régionaux afin de développer des moyens efficaces de promotion des normes internationales de protection des données et de la vie privée.

La résolution donnait mandat à l'Autorité Espagnole de Protection des Données, en tant qu'hôte de la 31ème Conférence internationale, pour créer et coordonner un groupe de travail composé des autorités intéressées, afin de rédiger et soumettre à la conférence, lors de sa session fermée, **une Proposition Conjointe pour l'établissement de Normes Internationales sur la Vie Privée et la Protection des Données Personnelles.**

La résolution comprenait une liste de critères déterminant la procédure de rédaction de cette Proposition Conjointe, et indiquait notamment que celle-ci devait être développée en encourageant une large participation des organisations publiques et privées, dans le but d'aboutir au plus large consensus institutionnel et social.

En accord avec ce mandat, l'autorité espagnole de protection des données a créé le groupe de travail visé dans la résolution et a promu et coordonner le travail d'élaboration de la Proposition Conjointe pour l'établissement de Normes Internationales.

L'autorité espagnole de protection des données a invité toutes les autorités accréditées à la Conférence Internationale à participer au groupe de travail. Les autorités listées en annexe 2 ont contribué aux travaux de ce groupe.

Le groupe de travail s'est réuni en janvier et juin 2009. La première réunion a permis de définir une méthodologie de rédaction de la proposition conjointe et sa portée, alors que la deuxième réunion a permis de discuter de la première version avancée, avant soumission à la 31ème Conférence.

Comme le prévoyaient les critères et la méthodologie définis dans la résolution de Strasbourg et acceptés par la groupe de travail, l'Autorité Espagnole de Protection des Données a mené les travaux d'élaboration des différents documents, qui incluent les contributions des autorités de protection des données et de la vie privée mais également d'autres organismes publics liés à la protection des données, ainsi que celles d'experts de l'industrie, des milieux juridique ou universitaire, d'organisations internationales et d'ONG.

Le groupe de travail a plus particulièrement rédigé une **Proposition Conjointe pour un Projet de Normes Internationales sur la Protection de la Vie Privée au regard du Traitement de Données Personnelles**,, en se fondant sur les principes présents dans plusieurs instruments, lignes directrices ou recommandations de portée internationale et qui ont obtenu un large consensus au sein des différentes zones géographiques, économiques ou juridiques.

La Proposition Conjointe a été rédigée en assumant que tous ces principes et approches communes apportent des éléments de valeur dans la défense et l'amélioration de la protection de la vie privée et des données personnelles, dans le but de les développer et d'y ajouter des solutions et des dispositions spécifiques, lesquels pourront s'appliquer quelque soient les différences qui peuvent exister entre les divers modèles de protection des données personnelles et de la vie privée.

Annexe 1 :

Proposition commune pour un projet de normes internationales sur la vie privée

1ère Partie : Dispositions générales

1. Objet

1. L'objet du présent Document est de:

a) définir un ensemble de principes et de droits garantissant une protection internationale uniforme et efficace en relation avec le traitement de Données Personnelles ; et

b) faciliter les transferts internationaux de Données Personnelles nécessaires dans un monde globalisé.

2. Définitions

Dans le cadre du présent Document :

a) "Données Personnelles" s'entend de toute information concernant une personne physique identifiée ou identifiable par des moyens dont l'utilisation est raisonnablement plausible.

b) "Traitement" s'entend de toute opération ou série d'opérations appliquées, automatisées ou non, sur des Données Personnelles, telles que la collecte, le stockage, l'utilisation, la divulgation ou la suppression.

c) "Personne concernée" s'entend de la personne physique dont les Données Personnelles sont sujettes à Traitement.

d) "Personne Responsable" s'entend de toute personne physique ou organisation, publique ou privée qui, seul ou conjointement, décide du Traitement.

e) "Prestataire de Services" s'entend de toute personne physique ou organisation, autre que la Personne Responsable, qui met en œuvre le Traitement de Données Personnelles pour le compte de ladite Personne Responsable.

3. Champ d'application

1. Ce Document vise dans son application tout Traitement de Données Personnelles, automatisé en tout ou en partie, ou sinon de manière organisée, et mis en œuvre par les secteurs public ou privé.

2. La loi nationale applicable peut établir que les dispositions de ce Document ne s'appliquent pas au Traitement de Données Personnelles effectué par une personne physique exclusivement dans le cadre de ses activités personnelles ou familiales.

4. Mesures additionnelles

1. Les Etats peuvent compléter le niveau de protection prévu dans ce Document avec des mesures additionnelles garantissant une meilleure protection de la vie privée au regard du Traitement de Données Personnelles.

2. Dans tous les cas, les dispositions de ce Document doivent être une base appropriée pour permettre les transferts internationaux de Données Personnelles, lorsque ces transferts sont menés conformément à l'Article 15 de ce Document.

5. Restrictions

Les Etats peuvent limiter le champ d'application des dispositions prévues aux articles de 7 à 10 et de 16 à 18 de ce Document, lorsque cela s'avère nécessaire dans une société démocratique, dans l'intérêt de la sécurité nationale, de la sûreté publique, pour la protection de la santé publique ou pour la protection de droits et libertés de tiers. De telles dérogations doivent être expressément prévues par la loi nationale, qui devra établir des garanties et limites appropriées destinées à préserver les droits de la Personne Concernée.

2ème Partie : Principes de base

6. Principe de licéité et de loyauté

1. Les Données Personnelles doivent être traitées loyalement, dans le respect de la loi nationale applicable et également des droits et libertés des individus, conformément au présent Document et en conformité avec les objectifs et principes de la Déclaration Universelle des Droits de l'Homme et du Pacte international relatif aux droits civils et politiques.

2. En particulier, tout Traitement de Données Personnelles qui donne lieu à une discrimination illégale ou arbitraire à l'encontre de la Personne Concernée doit être considérée comme injuste**.**

7. Principe de détermination des finalités

1. Le Traitement de Données Personnelles devrait être limité à la réalisation des finalités spécifiques, explicites et légitimes de la Personne Responsable.

2. La Personne Responsable ne devrait pas mettre en œuvre un Traitement qui serait incompatible avec les finalités pour lesquelles les Données Personnelles ont été collectées, à moins d'avoir obtenu le consentement non-ambigu de la Personne Concernée.

8. Principe de proportionnalité

1. Le Traitement de Données Personnelles devrait être limité aux Traitements adéquats, pertinents, et non-excessifs au regard des finalités fixées dans l'article précédent.

2. En particulier, la Personne Responsable devrait faire des efforts raisonnables pour limiter le Traitement de Données Personnelles au minimum nécessaire.

9. Principe de qualité des données

1. La Personne Responsable devrait en tout temps s'assurer que les Données Personnelles sont exactes, suffisantes et tenues à jour de telle sorte qu'elles remplissent les finalités pour lesquelles elles sont traitées.

2. La Personne Responsable devra limiter la durée de conservation des Données Personnelles traitées au minimum nécessaire. Ainsi, lorsque les Données Personnelles ne sont plus nécessaires pour atteindre les finalités qui ont légitimé leur Traitement, elles doivent être effacées ou rendues anonymes.

10. Principe de transparence

1. Chaque Personne Responsable devra avoir une politique transparente en relation avec le Traitement de Données Personnelles.

2. La Personne Responsable devra fournir aux Personnes Concernées, au minimum, des informations sur son identité, sur la finalité envisagée du traitement de leurs Données Personnelles, sur les destinataires à qui leurs Données Personnelles seront divulguées et sur les moyens d'exercer les droits que leur confère le présent Document, ainsi que toute autre information nécessaire pour garantir un Traitement loyal desdites Données Personnelles.

3. Lorsque les Données Personnelles ont été collectées directement auprès de la Personne Concernée, l'information doit être fournie au moment de la collecte, à moins qu'elle n'ait été fournie auparavant.

4. Lorsque les Données Personnelles n'ont pas été collectées directement auprès de la Personne Concernée, la Personne Responsable doit également le renseigner sur l'origine des Données Personnelles. Cette information doit être fournie dans un délai raisonnable, mais peut être remplacée par des mesures alternatives si la conformité est impossible ou implique un effort disproportionné de la part de la Personne Responsable.

5. Toute information à fournir à la Personne Concernée doit être fournie dans une forme intelligible, utilisant un langage clair et simple, en particulier lorsqu'il s'agit de Traitement adressé spécifiquement à des mineurs.

6. Lorsque les Données Personnelles sont collectées en ligne par des réseaux de communication électronique, les obligations exposées aux premier et second paragraphes du présent Article peuvent être remplies par la publication de chartes de protection de la vie privée facilement accessibles et identifiables et incluant tous les contenus ci-dessus mentionnés.

11. Principe de « Accountability »

La Personne Responsable doit :

a) Prendre toutes les mesures nécessaires pour observer les principes et obligations exposés dans le présent Document et dans la législation nationale applicable, et

b) Avoir les mécanismes internes en place pour démontrer l'observation des principes aux Personnes Concernées et aux autorités de contrôle dans l'exercice de leurs pouvoirs, comme prévu à l'Article 23.

3ème Partie : Légitimité du Traitement

12. Principe général de légitimité

1. D'une manière générale, les Données Personnelles ne peuvent être traitées que dans l'une des situations suivantes :

a) Après obtention du consentement libre, non ambigu et éclairé de la Personne Concernée ;

b) Lorsque l'intérêt légitime de la Personne Responsable justifie le Traitement, dès lors que les intérêts légitimes, droits et libertés de la Personne Concernée ne prévalent pas ;

c) Lorsque le Traitement est nécessaire au maintien ou à l'exécution d'une relation juridique entre la Personne Responsable et la Personne Concernée ; ou

d) Lorsque le Traitement est nécessaire pour être en conformité avec une obligation imposée à la Personne Responsable par la législation nationale applicable, ou est mené par une autorité publique dans l'exercice de ses pouvoirs.

e) Quand il existe des circonstances exceptionnelles qui menacent la vie, la santé ou la sécurité de la Personne Concernée ou d'une autre personne.

2. La Personne Responsable devra mettre en place des procédures simples, rapides et efficaces pour permettre aux Personnes Concernées de retirer leur consentement à tout moment. Lesdites procédures ne devront pas entraîner de délais ou coûts injustifiés, ni de bénéfices quelconques pour la Personne Responsable.

13. Traitement de données sensibles

1. Les Données Personnelles suivantes doivent être considérées comme sensibles :

- Données appartenant à la sphère la plus intime de l'individu, ou
- Données susceptibles de donner lieu, en cas de mauvaise utilisation, à :
    i. une discrimination illégale ou arbitraire, ou
    ii. un risque sérieux à la Personne Concernée.

2. En particulier, ces Données Personnelles qui peuvent révéler des aspects tels que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ; les données liées à la santé ou à la vie sexuelle seront considérées comme des données sensibles. La loi nationale applicable peut prévoir d'autres catégories de données sensibles lorsque les conditions énumérées dans le paragraphe précédent sont remplies.

3. Des garanties sérieuses doivent être établies pour préserver les droits des Personnes Concernées par la loi nationale applicable, qui doit prévoir des conditions additionnelles pour traiter des Données Personnelles Sensibles.

14. Prestations de services

La Personne Responsable peut réaliser le Traitement de Données Personnelles par l'intermédiaire d'un ou plusieurs Prestataires de Services, sans que cela soit considéré comme une divulgation de données à un tiers, à condition que :

a) La Personne Responsable s'assure que le Prestataire de Services garantit, au moins, le niveau de protection contenu dans ce Document et dans la loi nationale applicable ; et

b) La relation juridique est établie par un contrat ou un instrument juridique permettant de prouver son existence, sa portée et son contenu, et qui pose l'obligation du Prestataire de Services de se conformer à ces garanties et de s'assurer que les Données Personnelles sont traitées conformément aux instructions de la Personne Responsable.

15. Transferts internationaux

1. D'une manière générale, des transferts internationaux de Données Personnelles peuvent être réalisés lorsque l'Etat qui reçoit communication de telles données offre, au minimum, le niveau de protection prévu dans le présent Document.

2. Il sera possible de procéder à des transferts de Données Personnelles vers des Etats qui n'offrent pas ce niveau de protection prévu dans ce Document lorsque ceux qui prévoient de transférer de telles données garantissent que le destinataire offre un tel niveau de protection ; de telles garanties peuvent par exemple résulter de clauses contractuelles appropriées. En particulier, lorsque le transfert est effectué au sein d´entreprises ou de groupes multinationaux, de telles garanties peuvent être incluses dans des règles internes de protection de la vie privée, dont le respect est obligatoire.

3. En outre, la loi nationale applicable à ceux prévoyant de transférer des données peut permettre un transfert international de Données personnelles vers des Etats qui n'offrent pas le niveau de protection prévu dans ce Document, lorsque cela est nécessaire et dans l'intérêt de la Personne Concernée dans le cadre d'une relation contractuelle, pour protéger les intérêts vitaux de la Personne Concernée ou d'une autre personne, ou lorsque cela est requis par la loi sur la base d'un intérêt public important.

4. La loi nationale applicable peut conférer des pouvoirs aux autorités de supervision mentionnées à l'Article 23, d'autoriser certains ou tous les transferts internationaux tombant sous leur compétence, avant qu'ils soient mis en œuvre. Dans tous les cas, ceux qui prévoient de procéder à des transferts internationaux de Données Personnelles devraient être capable de démontrer que les transferts sont conformes aux garanties prévues dans ce Document, et en particulier lorsque cela est requis par les autorités de supervision conformément aux pouvoirs prévus à l'Article 23.2.

4ème Partie : Droits des Personnes Concernées

16. Droit d'accès

1. La Personne Concernée a le droit d'obtenir, à sa demande, auprès de la Personne Responsable des informations sur les Données Personnelles spécifiques sujettes à Traitement, ainsi que sur l'origine desdites données, les finalités du Traitement et les destinataires ou catégories de destinataires auxquels lesdites données sont ou seront divulguées.

2. Toute information qui sera communiquée à la Personne Concernée devra être fournie de façon intelligible, dans un langage clair et simple.

3. La législation nationale applicable peut limiter l'exercice répété de ce droit qui contraindrait la Personne Responsable à répondre à de multiples demandes sur de courtes périodes, à moins que la Personne Concernée ne justifie d'un intérêt légitime fierait.

17. Droit de rectification et d'effacement

1. La Personne Concernée a le droit de demander à la Personne Responsable l'effacement ou la rectification de Données Personnelles qui pourraient être incomplètes, inexactes, non nécessaires ou excessives.

2. Lorsque c'est justifié, la Personne Responsable pourra effectuer la modification ou l'effacement demandé. La Personne Responsable devra également en aviser les tiers auxquels des Données Personnelles auraient été divulguées, lorsque ils sont connus.

3. L'effacement n'est pas justifié lorsque des Données Personnelles doivent être conservées pour l'exécution d'une obligation imposée à la Personne Responsable par la législation nationale applicable, ou éventuellement par les relations contractuelles entre la Personne Responsable et la Personne Concernée.

18. Droit d'opposition

1. La Personne Concernée peut s'opposer au Traitement de ses Données Personnelles s'il existe un motif légitime résultant de sa situation personnelle spécifique2. L'exercice de ce droit d'opposition ne saurait être justifié lorsque le Traitement est nécessaire à la réalisation d'une obligation imposée à une Personne Responsable par le droit national applicable.

3. Toute Personne Concernée peut également s'opposer aux décisions qui produisent un effet juridique sur la seule base du Traitement automatisé de Données Personnelles, sauf dans les cas où la décision a été spécifiquement requise par la Personne Concernée ou lorsqu'elle est nécessaire à l'établissement, au maintien ou à l'exécution d'une relation juridique entre la Personne Responsable et la Personne Concernée. Dans ce dernier cas, la Personne Concernée doit être en mesure de revendiquer son point de vue afin de défendre ses droits ou intérêts.

19. Exercice de ces droits

1. Les droits prévus aux articles 16 à 18 du présent Document peuvent être exercés :

a) Directement par la Personne Concernée, qui devra dûment prouver son identité à la Personne Responsable.

b) Par l'intermédiaire d'un représentant, qui devra dûment prouver son statut à la Personne Responsable.

2. La Personne Responsable doit mettre en place des procédures pour permettre aux Personnes Concernées d'exercer les droits prévus aux paragraphes 16 à 18 du présent Document d'une manière simple, rapide et efficace qui n'entraîne pas de délai ou de coûts injustifiés, ni un quelconque gain au profit de la Personne Responsable.

3. Lorsqu'une Personne Responsable constate que, conformément à la législation nationale applicable, l'exercice des droits prévus dans cette Partie n'est pas admissible, la Personne Concernée devra être informée des raisons qui justifient ce constat.

5ème Partie : Sécurité

20. Mesures de sécurité

1. La Personne Responsable et le Prestataire de Services doivent tous deux protéger les Données Personnelles sujettes à Traitement par les mesures techniques et organisationnelles appropriées afin d'assurer en permanence leur intégrité, leur confidentialité et leur disponibilité. Ces mesures dépendent du risque existant, des conséquences possibles pour les Personnes Concernées, de la sensibilité du Traitement, de l'état de l'art, du contexte dans lequel le Traitement est mis en œuvre, et le cas échéant, des obligations prévues par la législation nationale applicable.

2. Ceux qui sont impliqués à un quelconque stade du Traitement doivent informer les Personnes Concernées de toute faille de sécurité susceptible d'affecter de manière significative leurs droits pécuniaires ou non pécuniaires, ainsi que des mesures prises pour sa résolution. Cette information devra être fournie en temps et en heure, pour permettre aux Personnes Concernées de rechercher la protection de leurs droits.

21. Devoir de secret

La Personne Responsable et ceux impliqués à un quelconque stade du Traitement de Données Personnelles devront en garder le secret. Cette obligation subsistera y compris après la fin de la relation avec la Personne Concernée ou, le cas échéant, avec la Personne Responsable.

6ème Partie : Conformité et surveillance

22. Mesures proactives

Les Etats, à travers leur législation nationale, pourront encourager la mise en œuvre, par ceux qui sont impliqués à un quelconque stade du Traitement, de mesures visant à promouvoir une meilleure conformité aux lois applicables sur la protection de la vie privée en relation avec le Traitement de Données Personnelles. De telles mesures pourraient inclure, entres autres:

a) La mise en œuvre de procédures de prévention et de détection des manquements, qui pourraient être basées sur les modèles standardisés de gouvernance de sécurité de l'information et/ou de gestion de la sécurité de l'information.

b) La nomination d'un ou plusieurs correspondants à la protection des données, dotés des qualifications, ressources et pouvoirs suffisants pour exercer leur fonction de supervision de manière adéquate.

c) La réalisation périodique de programmes de formation, d'éducation, de sensibilisation auprès des membres des organisations pour une meilleure compréhension des lois applicables sur la protection de la vie privée en relation avec le Traitement de Données Personnelles, ainsi que des procédures établies par les organisations à cet effet.

d) La réalisation périodique d'audits transparents, réalisés par des parties qualifiées et de préférence indépendantes afin de vérifier la conformité aux lois applicables sur la protection de la vie privée en relation avec le Traitement de Données Personnelles, ainsi qu'aux procédures établies par les organisations à cet effet.

e) L'adaptation des systèmes et/ou technologies de l'information pour le Traitement de Données Personnelles aux lois applicables sur la protection de la vie privée en relation avec le

Traitement de Données Personnelles, particulièrement au moment de décider de leurs spécifications techniques et de leur développement et mise en œuvre.

f) La mise en œuvre d'évaluations de l'impact sur la vie privée préalablement à la mise en œuvre de nouveaux systèmes et/ou technologies de l'information pour le Traitement de Données Personnelles, ainsi qu'avant la mise en place de nouvelles méthodes de Traitement de Données Personnelles, ou à toutes modifications substantielles dans le Traitement existant.

g) L'adoption de codes d'autorégulation contraignants, qui incluent des éléments permettant de mesurer leur efficacité en matière de conformité et de niveau de protection des données personnelles, et qui prévoient des mesures efficaces en cas de non-conformité.

h) La mise en œuvre d'un plan d'intervention établissant des lignes directrices d'action à prendre dans l'hypothèse d'un manquement aux lois applicables sur la protection de la vie privée en relation avec le Traitement de Données Personnelles, incluant au moins l'obligation de déterminer la cause et l'étendue du manquement, de décrire ses effets dommageables et de prendre les mesures appropriées pour éviter qu'il ne se reproduise dans le futur.

22. Surveillance

1. Dans chaque Etat, il devrait y avoir une ou plusieurs autorités qui, conformément à la législation nationale, seront chargées de superviser l'observation des principes établis dans le présent Document.

a) 2. Ces autorités devront être impartiales, indépendantes et auront des compétences techniques, et seront dotées de pouvoirs suffisants et de moyens adéquats pour gérer les plaintes déposées par les Personnes Concernées, et mener les contrôles et interventions nécessaires pour s'assurer de la conformité aux lois applicables sur la protection de la vie privée en relation avec le Traitement de Données Personnelles.

2. Dans tous les cas, et sans préjudice d'un recours administratif devant une autorité de contrôle visées dans les paragraphes précités, y compris d'un contrôle juridictionnel de leurs décisions, les Personnes Concernées devraient avoir un droit de recours direct devant les tribunaux pour faire respecter les droits qu'ils détiennent en vertu des dispositions de la législation nationale applicable.

23. Coopération et coordination

1. Les Autorités mentionnées au paragraphe précédent feront leurs meilleurs efforts pour coopérer les unes avec les autres en vue d'une meilleure uniformisation de la protection de la vie privée en relation avec le Traitement de Données Personnelles, aussi bien au niveau national qu'au niveau international. Afin de faciliter cette coopération, chaque Etat doit être en mesure, en cas de besoin, d'identifier l'autorité de contrôle territorialement compétente.

2. Ces autorités feront en particulier leurs meilleurs efforts pour :

a) Partager les rapports, techniques d'investigation, communication et stratégies de régulation et toute autre information utile à l'exercice plus efficace de leurs fonctions, en particulier à la suite d'une demande de coopération par une autorité de contrôle dans la conduite d'une investigation ou intervention ;

b) Conduire des investigations et interventions coordonnées, aussi bien au niveau national qu'au niveau international, dans les affaires où les intérêts de deux autorités ou plus sont partagés ;

c) Participer aux associations, groupes de travail et forums communs, de même qu'aux séminaires, ateliers ou cours qui contribuent à l'adoption de positions communes ou à

l'amélioration de la qualification technique du personnel au service de ces autorités de contrôle ;

d) Maintenir le niveau de confidentialité approprié pour ce qui est des informations échangées en application du présent article.

3. Les Etats doivent encourager la négociation d'accords de coopération entre autorités de contrôle, aussi bien régionales, nationales qu'internationales, qui contribuent à un respect plus efficace du présent article.

24. Responsabilité

1. La Personne responsable sera responsable des dommages et intérêts pécuniaires et non pécuniaires causés à la Personne Concernée à raison du Traitement de Données Personnelles en violation des lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, à moins que la Personne Responsable puisse démontrer que le dommage ne lui est pas imputable. Cette responsabilité est sans préjudice des actions que pourrait mener la Personne Responsable contre les Sous-traitants impliqués à l'une quelconque des étapes du traitement.

2. Les Etats promeuvent des mesures adéquates afin de faciliter l'accès des Personnes Concernées aux voies de recours judiciaires et administratives qui leur permettent d'obtenir réparation d'un dommage tel que mentionné dans le paragraphe précédent.

3. La responsabilité susmentionnée existera sans préjudice des sanctions pénales, civiles et administratives applicables en cas de violation du droit national relatif à la protection de la vie privée concernant le traitement des données personnelles.

4. La mise en place de mesures proactives telles que décrites à l'Article 22 de ce Document devra être considéré comme un élément déterminant la responsabilité et les pénalités prévues par le présent article.

Annexe 2 :
Autorités ayant participé au groupe de travail

Autorité de Protection des Données (Autriche)
Autorité de Protection des Données (Belgique)
Autorité de Protection des Données (Burkina-Faso)
Autorité de Protection des Données (Canada)
Autorité de Protection des Données (Canada -Québec)
Autorité de Protection des Données (République Tchèque)
Contrôleur Européen de la Protection des Données
Autorité de Protection des Données (France)
Autorité de Protection des Données (Allemagne)
Autorité de Protection des Données (Berlin - Allemagne)
Autorité de Protection des Données (Schleswig-Holstein - Allemagne)
Commissaire à la Protection des Données (Hong Kong)
Commissaire à la Protection des Données (Irlande)
Autorité de Protection des Données (Italie)
Autorité de Protection des Données (Pays-Bas)
Commissaire à la Protection des Données (Nouvelle-Zélande)
Autorité de Protection des Données (Portugal)
Commissaire à la Protection des Données (Slovénie)
Autorité de Protection des Données (Espagne)
Autorité de Protection des Données (Catalogne - Espagne)
Autorité de Protection des Données (Madrid – Espagne)
Autorité de Protection des Données (Pays basque – Espagne)
Commissaire à la Protection des Données (Suisse)
Commissaire à la Protection des Données (Grande-Bretagne)