OCDE

RAPPORT ANNUEL D'ACTIVITÉ DU COMMISSAIRE À LA PROTECTION DES DONNÉES

2019

Billy Hawkes

Janvier 2020

Table des matières

Introduction

Le présent document est mon premier rapport en tant que Commissaire à la protection des données (DPC) depuis ma nomination par le Secrétaire général, le 3 mai 2019. Il rend compte de la mise en œuvre, par l'Organisation, des règles révisées de l'OCDE en matière de protection des données, entrées en vigueur à cette même date, et fait le point sur les principaux domaines dans lesquels je suis intervenu au cours de ces premiers mois d'application, sur les actions de sensibilisation que j'ai menées, ainsi que sur le nombre de réclamations traitées et leurs principaux résultats. Il expose en outre les actions prévues en 2020 afin de poursuivre la consolidation du dispositif.

Version révisée des règles en matière de protection des données

L'OCDE a fait œuvre de pionnier en formulant des principes de protection de la vie privée et des données convenus au niveau international. Les *Lignes directrices de l'OCDE régissant la protection de la vie privée* ont jeté les bases de nombreux régimes nationaux et régionaux de protection des données. Elles conservent aujourd'hui toute leur pertinence et constituent le socle du nouveau dispositif interne de l'OCDE.

En tant qu'organisation intergouvernementale indépendante, l'OCDE n'est pas soumise aux législations nationales ou régionales. Pour ce qui concerne la protection des données, elle s'est dotée de ses propres règles internes, énoncées dans la *Décision du Secrétaire général relative à la protection des individus à l'égard du traitement de leurs données personnelles* (ci-après dénommée la « Décision » ou les « Règles »). Entrée en vigueur le 3 mai 2019, la Décision décrit les modalités de mise en œuvre des principes exposés dans les *Lignes directrices régissant la protection de la vie privée* au sein de l'Organisation. Elle tient également compte des évolutions récentes de l'environnement législatif en matière de protection des données. De plus, elle met à profit l'expérience acquise dans le cadre de la mise en œuvre du précédent dispositif interne de protection des données, qu'elle remplace, et aligne les dispositions relatives à la protection des données à caractère personnel à l'OCDE sur les normes les plus élevées en la matière.

Principes phares énoncés dans les Règles

Les Règles fixent un cadre complet régissant le traitement des données à caractère personnel par l'OCDE ou pour son compte. Les données concernées sont celles relatives aux membres du personnel de l'OCDE, aux délégués et visiteurs, et aux individus intervenant dans les projets de l'Organisation.

La *responsabilité* est un principe essentiel qui sous-tend les Règles, les « Coordinateurs » – à savoir les Directeurs et les responsables d'entités – étant chargés de la bonne gestion des données à caractère personnel au sein de leurs Directions et entités respectives. Les Règles présentent un certain nombre de caractéristiques fondamentales, dont des principes applicables au traitement des données, des dispositions relatives à l'exercice des droits des individus, et des mécanismes de mise en œuvre et de surveillance.

Principes applicables au traitement des données

La Décision, qui s'applique au traitement de l'ensemble des données à caractère personnel par l'Organisation ou pour son compte, exige que lesdites données soient :

- traitées de manière transparente et à des fins spécifiques, explicites et légitimes pour l'exécution par l'Organisation de sa mission et de son Programme de travail ;

- appropriées, pertinentes, exactes, raisonnablement tenues à jour, et limitées aux éléments nécessaires aux finalités de leur traitement ;
- traitées dans des conditions de sécurité suffisantes, en ayant recours, dans la mesure du possible et du raisonnable, à des mesures techniques ou structurelles adaptées ; et
- conservées pendant une durée ne dépassant pas celle qui est nécessaire au regard des finalités de leur traitement.

Aux termes de la Décision, le traitement de données personnelles sensibles et le traitement automatisé, y compris le profilage, sont soumis à d'importantes restrictions. De même, les traitements présentant des risques élevés font l'objet de mesures de protection particulières.

Droits des individus

La Décision reconnaît également aux individus des droits sur les données personnelles les concernant, qu'ils peuvent faire valoir directement auprès du Coordinateur.

Droits des individus

Transparence et information

– Les informations relatives au traitement des données sont consultables sur les sites intranet et/ou internet de l'Organisation.
– Les informations relatives au traitement des données peuvent être communiquées individuellement aux personnes qui en font la demande.

Droit d'accès

– Les individus ont la possibilité de savoir si des données personnelles les concernant font l'objet d'un traitement et disposent d'un droit d'accès à ces données.

Droit de rectification et droit à l'effacement

– Les individus peuvent demander à ce que des données personnelles inexactes les concernant soient rectifiées ou complétées.
– Les individus peuvent demander l'effacement des données personnelles les concernant.

Droit d'opposition

– Les individus ont le droit de s'opposer à un traitement qui ne serait pas nécessaire à l'exécution de la mission de l'OCDE.

Droit à la portabilité des données

– Les individus ont le droit d'obtenir les données les concernant et de les réutiliser pour des services différents.

Cadre de mise en œuvre

La conformité et la mise en place des mesures techniques et structurelles appropriées relèvent de la responsabilité des Coordinateurs. Le Délégué à la protection des données (DPO) doit être consulté préalablement à l'instauration ou au renouvellement de toute activité de traitement de données. Il est obligatoire de procéder à une évaluation des risques, la protection des données devant être intégrée dès la conception et par défaut au processus, de manière à garantir une prise en compte en amont des questions de protection des données et de la vie privée.

Des mesures techniques et structurelles adaptées doivent être prises afin de garantir un niveau de sécurité raisonnable et proportionné au risque. Les violations de données à caractère personnel doivent être signalées au Commissaire à la protection des données (DPC) et au Délégué à la protection des données (DPO) sous 48 heures, et aux personnes concernées dans un délai raisonnable.

Nomination du DPO et du DPC

La Décision a donné lieu à la création de deux nouvelles fonctions au sein de l'OCDE : celle de Délégué à la protection des données et celle de Commissaire à la protection des données. Tous deux sont chargés d'aider à la mise en œuvre des Règles par l'OCDE. Après avoir assumé la fonction de DPO par intérim, Michael Donohue a été nommé officiellement à ce poste par le Secrétaire général, à l'issue d'un appel à candidatures ouvert. J'ai pour ma part été nommé au poste de DPD pour une durée de cinq ans. Le DPO a notamment pour mission de concourir à la mise en œuvre au jour le jour des Règles, tandis que le DPC assure essentiellement un rôle de surveillance externe, y compris pour ce qui est des mesures d'application, en tant que de besoin. Une description sommaire de ces fonctions, dont la Décision donne le détail, est proposée ci-après.

Délégué à la protection des données

Mandat

- Expert de la réglementation, des politiques et des pratiques en matière de protection des données
- Agent de l'OCDE relevant directement du Secrétaire général
- Exerce ses fonctions en toute neutralité et indépendance

Responsabilités

- Fournir des informations et des conseils sur la Décision aux membres du personnel de l'OCDE et aux sous-traitants
- Promouvoir la sensibilisation et la formation des membres du personnel
- Fournir des informations et des conseils aux individus concernant le traitement des données personnelles les concernant et l'exercice de leurs droits aux termes de la Décision
- Prendre des mesures afin de garantir le respect de la Décision
- Vérifier tout traitement
- Prendre la décision de suspendre temporairement un traitement en cas de risque élevé
- Fournir des informations et prêter son concours au DPC

Commissaire à la protection des données

Mandat

- Veille à la mise en œuvre et au respect de la Décision
- S'acquitte de son mandat en toute indépendance et neutralité
- Est nommé par le Secrétaire général pour une durée de cinq ans

Responsabilités

- Formuler des avis sur le risque en matière de protection des données et aider à sa gestion
- Examiner les réclamations faisant état de violations des règles
- Informer les Coordinateurs de toute violation des règles

Pouvoirs d'enquête et de mise en place de mesures correctives

- Informer les personnes concernées en cas de violation de données personnelles
- Rectifier ou effacer des données à caractère personnel, ou en restreindre le traitement
- Suspendre, limiter ou interdire un traitement
- Formuler, à l'intention du Secrétaire général, des observations en vue de garantir la protection des données à caractère personnel
- Remettre un rapport d'activité annuel au Secrétaire général

Activités menées en 2019

Introduction

Au cours des sept mois qui ont suivi l'entrée en vigueur des Règles, la priorité a été de mettre à profit le solide cadre de protection de la vie privée déjà en place au sein de l'OCDE. Des efforts particuliers ont été déployés afin d'informer les parties prenantes internes et externes des exigences les plus impérieuses énoncées dans les Règles et de veiller à ce qu'elles soient intégrées aux procédures et protocoles opérationnels standard. Pour ce faire, une coopération étroite a été établie avec la Direction exécutive, en particulier avec le Bureau de la sécurité numérique, dont le rôle a été récemment renforcé, et avec la Direction des affaires juridiques. L'accent a également été mis sur le maintien de la sécurité des transferts de données entre l'OCDE et ses Membres.

Cartographie des données

L'établissement d'un inventaire de l'ensemble des activités de traitement des données à caractère personnel à l'échelle de l'Organisation constitue une étape importante de la conception et de la gestion d'un programme de protection des données. Cette démarche est nécessaire à deux titres : veiller à la mise en place de protections adaptées et être en mesure d'apporter des réponses appropriées aux demandes des individus au titre de l'exercice de leurs droits.

Un outil a été mis au point pour aider au processus de cartographie : le formulaire de traitement de données personnelles, mis à disposition sur l'intranet. Ce formulaire aide les Coordinateurs à mener à bien leurs missions de communication d'informations, de consultation préalable et d'évaluation des risques. Pour les projets impliquant de nouvelles demandes informatiques, des questions du formulaire ont été intégrées à un formulaire de demande plus large couvrant les besoins informatiques et les questions de sécurité, pour un traitement coordonné.

Les résultats préliminaires de l'activité de cartographie montrent que jusqu'à présent, l'OCDE procède au traitement des données à caractère personnel dans le cadre de l'exécution de sa mission, à des fins qui peuvent être regroupées dans trois grandes catégories :

1. Dans le cadre de son processus de recrutement, pour la gestion de ses ressources humaines et le versement des prestations aux membres de son personnel.
2. Pour faciliter la participation des délégués et d'autres personnes aux réunions officielles, manifestations et projets, et permettre l'accès aux sites web, communications et publications de l'OCDE.
3. Pour produire des données probantes à l'appui du processus d'élaboration des politiques.

Les traitements liés aux ressources humaines relevant de la première catégorie sont courants dans de nombreuses organisations de la taille de l'OCDE. Les données traitées dans le cadre de son rôle en tant que forum d'échanges pour les représentants officiels et les experts concernent essentiellement les coordonnées professionnelles et les détails de leurs interactions avec l'OCDE.

Les activités de traitement relevant de la troisième catégorie peuvent s'avérer plus complexes. Pour certains projets, les données à caractère personnel sont recueillies directement auprès des individus concernés (par exemple via l'outil Comparez vos revenus) ou par l'intermédiaire d'un prestataire de services travaillant pour l'OCDE (dans le cadre par exemple de l'enquête Des risques qui comptent). Pour d'autres projets relevant de la troisième catégorie, des données à caractère personnel sont collectées par les Membres, puis transmises à l'OCDE ou à ses sous-traitants. Dans ce cas, les Membres doivent se conformer à leur propre législation nationale en matière de protection des données ; en règle générale, seules des données dépersonnalisées sont transférées. Ces projets peuvent être de différents types ; quelques exemples en sont donnés ci-après.

Exemples de projets impliquant l'obtention de données à caractère personnel auprès d'administrations publiques ou de tierces parties

- *Programme international pour le suivi des acquis des élèves* (PISA) (enquête visant à évaluer la capacité des jeunes de 15 ans à mobiliser leurs connaissances et leurs compétences en lecture, en mathématiques et en sciences)
- *Programme pour l'évaluation internationale des compétences des adultes* (PIAAC) (enquête destinée à évaluer les compétences clés des adultes en matière de traitement de l'information)
- *Enquête internationale sur l'enseignement et l'apprentissage* (TALIS) (enquête réalisée auprès d'enseignants et de chefs d'établissement sur les conditions d'exercice de leur métier et l'environnement d'apprentissage)
- *Étude sur les compétences sociales et émotionnelles* (enquête réalisée auprès des jeunes de 10 et de 15 ans dans le but d'évaluer les conditions et les pratiques ayant une influence sur le développement des compétences sociales et émotionnelles)
- *Étude internationale sur l'apprentissage et le bien-être des jeunes enfants* (IELS) (enquête portant sur les enfants âgés de 5 ans, dans trois pays, et destinée à identifier les principaux déterminants du développement de leur apprentissage)
- *Enquête sur les indicateurs fondés sur les déclarations des patients* (PaRIS) (enquête sur le vécu des personnes atteintes d'une maladie chronique et soignées dans des structures de soins primaires ou ambulatoires)
- *Données sur la mise en œuvre et le suivi de la Convention anticorruption* (données sur les procédures pénales, administratives et civiles pour des faits de corruption transnationale)

Beaucoup reste à faire pour finaliser la cartographie de l'ensemble des données détenues par l'Organisation, et l'inventaire qui en résultera devra être mis à jour régulièrement, à mesure que des projets arriveront à leur terme et que d'autres seront lancés. L'exercice de cartographie présente des liens avec les efforts déployés au sein du Bureau de la sécurité numérique, ainsi qu'avec une enquête réalisée par la Direction des statistiques et des données sur les projets de l'OCDE impliquant la production de statistiques et de données.

Information/Sensibilisation

La transparence étant un élément fondamental de la protection des données et de la vie privée, la Décision intègre un certain nombre de dispositions en ce sens.

Intranet/Internet

La publication de la Décision sur les sites intranet et internet de l'OCDE était une condition préalable à son entrée en vigueur, au mois de mai. Une nouvelle page interne a été créée sur l'intranet : elle contient une description de la Décision et le lien pour la consulter. De plus, la page Politique de protection des données et de la vie privée a été actualisée en mai de manière à faire référence à la nouvelle Décision.

Plus tard, une nouvelle page de présentation générale a été ajoutée au site public afin de donner des informations sur l'approche interne de l'OCDE en matière de protection des données dans le cadre de ses activités. Au titre d'une approche « multiniveau » de la communication d'informations aux individus, des notes d'information spécifiques sont préparées pour diverses activités ; elles sont accessibles à partir de la page de présentation. La politique de protection des données et de la vie privée couvre la collecte des données concernant les visiteurs qui consultent le site web de l'OCDE. À

cela s'ajoute une note spécifique pour le recrutement, dans laquelle la référence à la Décision a été mise à jour.

Des travaux complémentaires sont en cours pour renforcer les efforts de communication par le biais de l'élaboration de notes d'information sur la protection des données. Le DPO a créé à cet effet un modèle que les membres du personnel peuvent utiliser comme point de départ afin de s'assurer que tous les éléments requis figurent dans leur note. Par exemple, une note en cours de préparation vise à donner des informations sur le traitement des données concernant les délégués et d'autres visiteurs qui viennent à l'OCDE. Les entités et organes œuvrant dans le cadre de l'Organisation (à l'instar de l'AIE, de l'AEN et du FIT) ont également entrepris d'actualiser les politiques de protection de la vie privée publiées sur leurs sites web respectifs afin d'y faire référence à la Décision. Ces initiatives ont été facilitées par la préparation d'un modèle de politique de protection de la vie privée destiné à favoriser la cohérence et la clarté des notes d'information ainsi mises à jour.

Des efforts sont par ailleurs déployés en vue d'élaborer des notes propres à certains projets, lorsque nécessaire. La mise au point d'une nouvelle application mobile destinée à être utilisée par les participants aux conférences a ainsi nécessité la rédaction d'une note d'information ciblée. Des informations supplémentaires sont en outre ajoutées aux sites dédiés aux conférences lorsque sont menées des activités dépassant le cadre des traitements de données décrits dans les notes d'information plus générales (pour indiquer par exemple qu'un événement doit être diffusé sur le web).

Guides pratiques à l'intention des membres du personnel

Le DPO a préparé une nouvelle série de guides pratiques dans lesquels sont exposés des conseils quant à la mise en œuvre de la Décision dans le cadre de diverses activités régulières. Ces guides sont publiés dans la section *How-to Guides* du site intranet et annoncés par différents canaux de communication, dont le *Conseil de la semaine* (*Tip of the Week*) et la lettre d'information *Les essentiels d'EXD*.

Guides pratiques sur la protection des données

- Comment traiter une demande de données personnelles
- Comment établir une notification sur la protection des données
- Comment traiter les listes de participants

L'expérience acquise au fil de la mise en œuvre des règles de protection des données fera émerger de nouveaux sujets qui viendront enrichir ces outils pratiques afin d'accroître la sensibilisation et de promouvoir les bonnes pratiques.

Engagement interne et visibilité

La meilleure stratégie pour renforcer la sensibilisation et veiller au respect des règles consiste à intégrer la protection des données dans les activités quotidiennes de l'Organisation. Pour ce faire, la priorité a été donnée, au cours des premiers mois de mise en œuvre des Règles, aux rencontres et aux échanges entre les membres du personnel et les DPC et DPO. En 2019, je me suis rendu à plusieurs

reprises[1] à l'OCDE, où j'ai rencontré le Secrétaire général, la Directrice du Cabinet et les responsables d'EXD et de LEG, ainsi que des agents des Directions de substance. J'ai également participé, avec le DPO, à une réunion du Groupe des Directeurs présidée par le Secrétaire général, dont l'un des points à l'ordre du jour était consacré à l'examen des Règles. Cette réunion a été l'occasion d'attirer l'attention des Directeurs sur leur rôle clé et leurs responsabilités au titre de la Décision.

Avec mon soutien, le DPO est devenu un membre régulier ou participant au sein d'un certain nombre de groupes de coordination à l'échelle de l'Organisation, parmi lesquels :

- Le groupe de coordination des technologies de l'information (*Information Technology Coordination Group*, ITCG)
- Le Groupe de gouvernance de la sécurité de l'information (*Information Security Governance Group*, ISGG)
- La Commission des statistiques et des données au niveau des managers (*Statistics and Data Board at Manager's level*, SDB-M)
- La Communauté de pratique des statistiques et des données sur les microdonnées
- Les Correspondants informatiques (CI).

Il a également été en relation avec le réseau des Conseillers en gestion des ressources (RMA), celui des Conseillers, ainsi que le Conseil de communications afin de nouer un dialogue régulier avec les personnes les mieux placées pour détecter les problématiques de protection des données qui peuvent se faire jour.

Une activité de sensibilisation menée conjointement avec le Bureau de la sécurité numérique est prévue le 28 janvier 2020, à l'occasion de la Journée internationale de la protection des données. Diverses actions seront alors menées : diffusion de messages à l'intention de l'ensemble des membres du personnel, lancement de plusieurs guides pratiques et deux débats en panel sur la façon dont une gouvernance solide des données peut faciliter l'accès aux sources de données nécessaires à l'élaboration des politiques. Je prendrai part aux débats, et j'espère à cette occasion intéresser le personnel à ces questions et montrer que de bonnes mesures de protection de la vie privée et de la sécurité non seulement sont essentielles à la protection des individus, mais aident également l'Organisation à mener à bien sa mission d'intérêt public.

Engagement externe et visibilité

Les Règles ont pour vocation première d'améliorer la capacité de l'Organisation de protéger les individus dans le cadre des activités ayant trait au traitement des données. Elles lui permettent en outre de mettre ses pratiques internes en adéquation avec le rôle qu'elle joue de longue date en tant que chef de file de l'élaboration de politiques publiques dans ce domaine. Qui plus est, l'obtention des données nécessaires à l'analyse des politiques est de plus en plus conditionnée par l'aptitude de l'Organisation à apporter des garanties de protection de la vie privée et de sécurité qui répondent aux exigences qu'imposent les sources de données externes. L'engagement externe et la visibilité constituent par conséquent des ingrédients essentiels à la réussite de la mise en œuvre des Règles.

Diverses activités d'ouverture ont été menées en 2019, dont des échanges avec la communauté des responsables de la protection des données dans d'autres organisations internationales et la communauté plus large des acteurs de la protection des données. Peu après l'entrée en vigueur des Règles, le DPO et moi-même nous sommes rendus à Bruxelles pour présenter les Règles aux agents

[1] Dates : 16 avril ; 20 et 21 mai ; 17 et 18 juin ; 9 juillet ; 29 octobre.

de la Commission européenne et engager un dialogue sur les questions de transferts internationaux de données évoquées ci-après.

Les 17 et 18 juin, l'OCDE a co-organisé avec le Contrôleur européen de la protection des données l'atelier annuel sur la protection des données dans les organisations internationales. Au cours de cet atelier, 90 participants représentant plus de 40 organisations ont débattu des défis communs que pose la mise en œuvre de la protection des données dans le cadre de leurs activités.

En octobre, je suis devenu membre de la Conférence mondiale sur la protection de la vie privée (*Global Privacy Assembly*, ou GPA, anciennement dénommée Conférence internationale des commissaires à la protection des données et de la vie privée) et j'ai pris part à sa 41e réunion, à Tirana, en Albanie. J'y ai été rejoint par le DPO et d'autres collègues de l'OCDE, qui y ont assisté en qualité d'observateurs. En marge de la conférence ont pu se tenir des réunions avec la Commission européenne et un certain nombre d'organismes de protection des données.

Formulation de conseils et consultation préalable

Le DPO a pour mission principale de conseiller le personnel sur ses responsabilités au regard des Règles ; je l'aide à mener à bien cette mission en participant à des échanges réguliers sur des questions particulières. En 2019, l'avis du DPO a été sollicité sur un grand nombre de projets menés à l'échelle de l'Organisation et des entités affiliées, pour diverses questions ayant trait à la protection des données. Le tableau ci-dessous propose une liste non exhaustive des sujets abordés lors de ces consultations.

Sélection de sujets abordés lors des consultations du DPO (2019)

Diffusion des réunions sur le web (webcasts) · traductions · coûts d'impression du personnel · outil d'aide aux déménagements de bureaux · quiz sur les plaques diplomatiques · enquête sur la culture · outil CRM · formation du personnel · contrat Centre de services · accès aux comptes des membres du personnel · enquêtes auprès des étudiants · enquêtes auprès des enseignants · application de gestion des événements · utilisation des données des experts · enquêtes sur la tolérance religieuse · enquête pour la collecte de microdonnées sur la santé · listes d'adresses électroniques · enquêtes auprès du personnel · listes de participants · enquête de consultation · création d'observatoire · utilisation du CV des membres du personnel · enquêtes auprès des parties prenantes · politique de protection de la vie privée sur les sites web · collecte de vidéos · enquête sur les revenus · enregistrement de conférence · transferts de données · listes de contacts · reporting relatif à la mise en œuvre de programmes

Violations de données

Deux cas de violations de données ont été signalés après l'entrée en vigueur des Règles. Dans le premier cas, un bulletin de pension n'a pas été mis à la disposition du bon bénéficiaire. Dans le second, les données fiscales concernant cinq retraités de l'OCDE ont été transmises à la mauvaise administration fiscale. Les deux incidents résultent d'une erreur humaine. Des mesures appropriées ont été prises pour que les données erronées soient supprimées, et pour informer les personnes concernées et réduire le risque que de telles erreurs se reproduisent.

Des actions de suivi ont en outre été menées pour un cas de violation de données à caractère personnel intervenu avant l'entrée en vigueur des Règles. L'incident n'était pas lié aux systèmes de l'OCDE, mais à des fichiers de coordonnées bancaires détenus par le gestionnaire de frais de santé de l'Organisation. Suite à cette violation de données, certains membres actuels et anciens du personnel de l'OCDE ont été victimes de prélèvements bancaires frauduleux. Le suivi réalisé par le DPO de l'OCDE a montré que le prestataire avait pris des mesures appropriées pour résoudre la faille de sécurité et avait coopéré à l'enquête menée par l'OCDE sur cet incident.

Demandes liées à l'exercice des droits des individus

Un protocole a été mis en place pour répondre aux demandes liées à l'exercice des droits des individus ; il est décrit dans un guide pratique qui doit être publié début 2020. Trois demandes liées aux droits énoncés dans la Décision ont été soumises en 2019, chacune ayant été satisfaite par l'Organisation.

- La première correspondait à une demande d'effacement, qui a donné lieu à la suppression d'un profil de candidat créé par le demandeur dans la base de données de l'OCDE relative aux recrutements.
- La deuxième (également une demande d'effacement) a donné lieu à la suppression du compte MyOECD du demandeur.
- La dernière demande concernait des données personnelles contenues dans une présentation, que le demandeur avait soumise à l'OCDE pour publication. La présentation a été retirée sans délai du site web de l'OCDE.

Réclamations et exercice des pouvoirs officiels

Aucune réclamation n'a été portée à ma connaissance ni à celle du DPO en 2019.

Aucune situation ne m'a conduit à exercer, en 2019, mes pouvoirs d'enquête ou de mise en place de mesures correctives au titre de la Décision.

Transferts internationaux de données aux termes du RGPD

L'un des problèmes majeurs auxquels l'Organisation a été confrontée concerne les transferts de données à caractère personnel provenant de Membres de l'EEE, requis dans le cadre de certains projets de l'OCDE. Les difficultés rencontrées tiennent au fait que les dispositions du Règlement général sur la protection des données (RGPD) de l'UE limitant de tels transferts s'appliquent aux organisations internationales. Le problème s'est posé, par exemple, pour les transferts nécessaires pour mener à bien d'importants projets comme le PISA et le PIAAC.

Ces difficultés ne sont pas liées à la question de savoir si les mesures de protection mises en place par l'OCDE au titre de ces programmes sont suffisantes pour parer à tout risque susceptible de peser sur les individus, ni à la solidité du dispositif de protection des données actuellement en vigueur à l'OCDE. Elles tiennent en revanche à l'interprétation de certaines exigences énoncées dans le RGPD, qui ne sont pas nécessairement adaptées au statut juridique ni à la portée internationale des organisations intergouvernementales comme l'OCDE.

Si l'OCDE n'est pas soumise au RGPD, ses Membres appartenant à l'EEE le sont. Pour les aider, j'ai participé, aux côtés du DPO et de la Direction des affaires juridiques, aux débats menés avec les autorités de l'UE compétentes, dont la Commission européenne, ainsi que plusieurs organismes nationaux chargés de la protection des données. Je suis satisfait de constater que les parties prenantes reconnaissent la nécessité de résoudre ces difficultés et ont la volonté de trouver des solutions

adaptées afin de faire en sorte que les flux de données nécessaires à la réalisation des importants travaux d'intérêt public de l'Organisation ne soient pas interrompus.

Plans pour 2020

Au cours de mes sept premiers mois d'exercice en tant que DPC, des progrès considérables ont été réalisés dans la mise en place des processus et des pratiques nécessaires à l'établissement d'un programme de protection des données de haut niveau à l'OCDE. Pour autant, beaucoup reste à faire pour affiner la mise en œuvre du nouveau dispositif.

Les priorités pour 2020 en termes de protection des données sont les suivantes :

- ***Cartographie des données*** : Il est essentiel de parvenir à une cartographie exhaustive des activités de traitement des données à caractère personnel pour permettre une évaluation correcte des risques par les Coordinateurs et une hiérarchisation des efforts pour les gérer. Des travaux supplémentaires devront être menés pour finaliser l'inventaire des usages des données à caractère personnel à l'échelle de l'Organisation et publier les résultats en toute transparence. Une attention particulière devra être portée aux activités de traitement sous-traitées à des tierces parties et à l'utilisation des applications infonuagiques. Le renforcement de la coordination avec les travaux menés parallèlement par le Bureau de la sécurité numérique sera bénéfique pour tous les acteurs.
- ***Notes d'information sur la protection des données*** : La mise en place de l'approche multiniveau de l'élaboration des notes d'information, adoptée en 2019, doit être étendue à l'ensemble des sites web et des activités menées actuellement au sein de l'OCDE et des autres organes œuvrant dans le cadre de l'Organisation.
- ***Sensibilisation et formation*** : Dans la droite ligne des activités organisées en janvier 2020 à l'occasion de la Journée internationale de la protection des données, des efforts supplémentaires devront être déployés afin de renforcer la sensibilisation aux Règles, en s'attachant en particulier à mettre en évidence la nécessité d'accroître la transparence sur le traitement des données relatives aux délégués et aux visiteurs. À cela s'ajoutera l'élaboration d'un plan en vue de la mise en place d'activités de formation intégrant, dans la mesure du possible, les questions de protection des données et de sécurité numérique, et organisé en coordination avec d'autres programmes de formation de l'OCDE.
- ***Gestion des incidents donnant lieu à une violation de données*** **:** Toutes les organisations doivent se préparer à gérer un incident de sécurité se traduisant par une violation de données à caractère personnel. Les Règles de l'OCDE prévoient des obligations de notification spécifiques. Reste désormais à formuler des orientations à l'intention des membres du personnel, en coopération avec le Bureau de la sécurité numérique.
- ***Transferts internationaux de données*** : Il convient de poursuivre les efforts afin d'aider les membres de l'EEE à relever les défis liés au respect des dispositions du RGPD relatives aux transferts de données à caractère personnel vers l'OCDE.

Ces priorités viennent s'ajouter aux activités courantes de conseil en matière de conformité et de bonnes pratiques, et de traitement des demandes d'exercice des droits individuels ou des réclamations. Au terme d'une première année de mise en œuvre des Règles, en mai 2020, nous devrions avoir acquis une expérience suffisante pour amorcer une réflexion sur le fonctionnement des Règles et vérifier si les ressources et les structures de gouvernance sont à la hauteur des enjeux.