Strasbourg, 21 mai 2024

DPCOM Rapport 2022-2024

Rapport d'activité
du Commissaire à la protection des données

novembre 2022 – juin 2024

Table des Matières

Avant-propos

Jamais depuis la chute du mur de Berlin, la menace d'un cataclysme irréversible n'a pesé de manière aussi virulente sur nos sociétés en Europe et dans le monde. Nous assistons à un recul de l'Etat de droit, de la démocratie et des droits humains, y compris du droit à la protection des données. Les guerres qui se déroulent sur le continent européen et dans d'autres régions du monde, ainsi que la persistance des menaces terroristes créent un climat négatif et d'insécurité qui favorise l'émergence de mouvements antidémocratiques et propres à remettre en cause les droits humains consacrés en particulier par la déclaration universelle des droits de l'homme et la Convention européenne des droits de l'Homme.

Nous assistons à une montée en puissance de politiques de surveillance au nom de la sécurité des personnes et des biens qui ne sont pas nécessairement proportionnées par rapport aux objectifs à atteindre. De nombreux gouvernements n'hésitent plus à mettre en place des systèmes de vidéosurveillance généralisés basés sur la reconnaissance faciale et la biométrie ou à recourir à des technologies de surveillance et de pistage non suffisamment ciblées des activités des personnes sur la toile entraînant notamment des risques non négligeables de discrimination et de stigmatisation. Il sied de rappeler que la sécurité des citoyennes et des citoyens ne peut se faire au détriment des droits humains et que les mesures mises en place doivent se faire en garantissant le droit à la protection des données.

Cette surveillance massive continue également à se développer par l'entremise de nombreux acteurs de l'économie numérique à travers la collecte sans limites de données que toutes et tous nous fournissons souvent de manière inconsciente ou irréfléchie lors de nos interactions numériques. L'exploitation de ces données à l'aide de l'Intelligence artificielle permet à ces acteurs de nous profiler et d'orienter nos actions, nos comportements et nos décisions. On ne le soulignera jamais assez, il est impératif de ne pas abandonner les pouvoirs de décision à quelques acteurs privés au risque de mettre définitivement à mal l'Etat de droit, les droits humains et la démocratie. Ces acteurs se doivent d'agir de manière transparente dans le respect des normes légales en vigueur de manière à rétablir la confiance dans le recours aux technologies de l'information et de communication. Nous devons ainsi œuvrer pour le développement de solutions axées sur une gouvernance plus démocratique des traitements de données et de leurs algorithmes. L'adoption le 17 mai par le Comité des Ministres de la Convention cadre sur l'Intelligence Artificielle et les droits de l'homme, la démocratie et l'Etat de droit, suivant ainsi l'adoption par l'Union européenne de son règlement de l'intelligence artificielle est un pas important à saluer.

L'année 2024 se trouve ainsi à la croisée des chemins. Même si les perspectives ne sont hélas pas des plus optimistes pour l'avenir, une lueur d'espoir existe avec la très probable entrée en vigueur de la Convention 108+ dans le courant de l'année, laquelle devrait apporter un nouvel élan à la protection des droits humains et des libertés fondamentales lors du traitement de données à caractère personnel.

Le Conseil de l'Europe qui renforce également sa sécurité et planifie le recours à l'intelligence artificielle, notamment dans le domaine des ressources humaines, ne peut se contenter de rechercher une meilleure efficacité, un accroissement de la productivité et une rationalisation des processus d'activités. Il se doit d'être un exemple dans la défense des valeurs qui sont les siennes, à savoir la défense de l'Etat de droit, de la démocratie et des droits humains lors du recours à des technologies nécessitant le traitement de données personnelles.

L'entrée en vigueur du nouveau règlement de protection des données offre ainsi un cadre propice à assurer la protection des personnes lors du traitement de données personnelles. Encore faut-il investir rapidement dans les ressources nécessaires pour garantir l'effectivité de la protection des données.

1. Introduction

Le mandat du Commissaire à la protection des données du Conseil de l'Europe a été initialement établi par le Règlement du Secrétaire Général du 17 avril 1989 instaurant un système de protection des données pour les fichiers de données à caractère personnel du Conseil de l'Europe. Par sa résolution CM/Res(2022)14, le Comité des Ministres a adopté le nouveau Règlement du Conseil de l'Europe sur la protection des données à caractère personnel.

Ce nouveau règlement est entré en vigueur le 1er janvier 2023, avec une période transitoire de deux ans pour l'Organisation[1].

Ainsi, selon la Résolution CM/Res (2022)14, le/la Commissaire à la protection des données, en fonction de la date d'entrée en vigueur du présent Règlement, continue d'exercer ses missions jusqu'à l'expiration de son mandat, sans préjudice de la possibilité d'être réélu(e) conformément aux dispositions du présent Règlement[2].

En attendant l'entrée en vigueur de la Convention 108+, le/la Commissaire à la protection des données est élu(e) par les représentants(es) des États membres au sein du Comité de la Convention établi en vertu de l'article 18 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Le Commissaire actuellement en fonction, Monsieur Jean Philippe Walter, a été élu lors de la 36ème réunion plénière du Comité consultatif de la Convention 108 (Strasbourg, 19-21 juin 2018) et réélu, sous l'ancien régime, en juin 2021 lors de la 41ème réunion plénière du Comité consultatif.

Le rapport d'activités du/de la Commissaire à la protection des données est également présenté au dit Comité de la Convention[3]. En vertu de l'Article 17 du nouveau Règlement, le/la Commissaire à la protection des données préparera et publiera un rapport annuel décrivant ses activités. Le rapport doit être présenté pour information au dit Comité de la Convention ; puis il est transmis à la Secrétaire Générale avant d'être rendu public. Le présent rapport couvre le période transitoire entre deux Règlements et fait état des activités menées entre novembre 2022 et juin 2024.

2. Règlement du Conseil de l'Europe sur la protection des données

Après quelques dix ans de travaux, le Conseil de l'Europe s'est doté d'une législation moderne en matière de protection des données avec l'adoption le 15 juin 2022 par le Comité des Ministres de la résolution CM/Res(2022)14 instituant le Règlement du Conseil de l'Europe sur la protection des données à caractère personnel. Comme indiqué dans l'introduction, ce nouveau règlement est entré en vigueur le 1er janvier 2023.

Le nouveau Règlement sur la protection des données poursuit deux objectifs principaux :

- relever les défis résultant de l'utilisation des nouvelles technologies de l'information et de la communication, et :
- améliorer la protection des données au sein du Conseil de l'Europe en renforçant les droits des individus et en leur donnant plus de contrôle sur leurs données personnelles.

Il est très important de souligner que ce règlement permet au Conseil de l'Europe de se mettre en grande partie en conformité avec la Convention 108+.

---

[1] Selon l'Article 2 de la Résolution CM/Res(2022)14 instituant le Règlement du Conseil de l'Europe sur la protection des données à caractère personnel, le/la Secrétaire Général(e) veille à ce que les traitements de données à caractère personnel déjà en cours à la date d'entrée en vigueur du présent Règlement soient mis en conformité avec celui-ci dans un délai de deux ans.

[2] Article 3 de ladite Résolution.

[3] Article 4 de ladite Résolution.

Le règlement a pour objectif d'assurer la protection de toute personne, quelle que soit sa nationalité ou son lieu de résidence, lors du traitement de données personnelles par les différentes instances et organes de l'Organisation et ainsi de respecter les droits humains et les libertés fondamentales, notamment le droit à la vie privée.

Ce règlement s'applique à tout traitement de l'Organisation effectué au siège à Strasbourg ou dans les différents bureaux extérieurs du Conseil de l'Europe. Il ne s'applique cependant pas aux traitements de la CEDH et du Tribunal administratif dans le cadre de leurs activités judiciaires. Ces traitements doivent être régis par les règles adoptées par ces deux instances judiciaires. En revanche les traitements ne relevant pas des activités judiciaires demeurent régis par le règlement. A noter que la CEB n'y est pas soumise et dispose de son propre règlement de protection des données.

Le règlement énonce les principes de base devant régir tout traitement (article 4), à savoir le respect :
- des principes de proportionnalité, de licéité, de loyauté et de transparence,
- du principe de finalité selon lequel les données ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes et ne sont pas traitées de manière incompatible avec ces finalités ;
- du principe d'adéquation, de pertinence et non excessivité ;
- du principe d'exactitude ;
- de conservation n'excédant pas ce qui est nécessaire à la finalité pour laquelle les données sont traitées.

Il fixe les conditions légitimant le traitement des données et en particulier le respect du principe de légalité (article 4.2).

Il énonce les droits des personnes concernées et notamment le droit d'accès, le droit à la transparence des traitements, le droit de rectification ou d'effacement des données, le droit de ne pas être soumis à une décision automatisée sans que la personne puisse faire valoir son point de vue, ainsi que le droit de disposer d'un recours effectif.

Le règlement définit les obligations des responsables de traitement, parmi lesquelles figure l'obligation de mise en conformité, de procéder à un examen de l'impact potentiel du traitement sur les droits et libertés fondamentales des personnes concernées, le respect des principes de *privacy by design* et par défaut, les obligations de transparence et d'annonce des violations de données.

Pour veiller au respect des dispositions en matière de protection des données, le règlement prévoit la mise en place au minimum d'un(e) délégué(e) à la protection des données (*DPO*) qui doit être impliqué(e) dans toutes les questions relatives à la protection des données. Le/la DPO est le premier point de contact avant de saisir le/la Commissaire à la protection des données.

L'institution du/de la Commissaire à la protection des données n'est pas nouvelle et était déjà en place sous l'ancien régime. Avec le nouveau règlement sa position, son rôle et ses pouvoirs sont renforcés.

Conformément à la Convention 108+, l'article 15 du règlement précise que le/la Commissaire est une autorité de contrôle indépendante chargée de veiller à la conformité des traitements de données à caractère personnel de l'organisation. Il jouit de pouvoirs d'intervention et d'investigation et notamment d'un pouvoir de décision. A ce titre, le/la Commissaire est chargé(e) notamment de :

- Contrôler et assurer l'application des dispositions du règlement.
- Examiner les réclamations des personnes concernées et ordonner les mesures correctives.
- Mener des enquêtes.
- Formuler des avis à la demande du/de la DPO.
- Faire des recommandations au/à la responsable de traitement.
- Coopérer avec les autorités nationales ou internationales de protection des données, y compris les organisations internationales.

Comme indiqué précédemment, il/elle doit également rédiger et publier un rapport annuel sur ces activités. En conformité avec la Convention 108+, il/elle devrait également pouvoir sensibiliser aux questions d'actualité en matière de protection des données et donner son avis sur les projets législatifs ou les propositions administratives impliquant des traitements de données à caractère personnel.

Enfin, le/la Commissaire se prononce sur les réclamations des personnes concernées et transmet ses conclusions qui sont définitives et contraignantes au/à la Secrétaire Générale qui doit décider sur cette base. La personne concernée peut recourir contre la décision au Tribunal administratif s'il s'agit d'un membre du personnel, d'un ancien membre du personnel, de ses ayants droit ou d'un candidat à un emploi. Pour les autres personnes qui contestent la décision, un accord à l'amiable doit être recherché et, en cas d'échec, le litige sera soumis à un arbitrage définitif et contraignant.

Les agents qui ne respectent pas le règlement de protection des données s'exposent à des sanctions disciplinaires.

Cependant, l'obligation de mise en conformité, notamment en procédant, avant tout traitement, à l'examen de l'impact potentiel dudit traitement sur les droits et les libertés fondamentales des personnes concernées ou l'obligation de consulter, lorsque requis, le/la DPO n'est pas encore suffisamment intégré(e) par les différents services concernés. Certaines entités ne sont pas encore conscientes de l'importance de la protection des données et mettent du temps à fournir les réponses demandées ou le font de manière incomplète, nécessitant des relances tant de la DPO, que du/de la Commissaire.

Pour être effectif, le Règlement doit être appliqué de manière éclairée. Ainsi, un effort conséquent et prioritaire doit être fait pour sensibiliser et former les agents de l'Organisation aux exigences en matière de protection des données.

3. Présence physique au siège de l'Organisation et représentation

3.1 Visites au Conseil de l'Europe

Le Commissaire à la protection des données a pu effectuer plusieurs visites de travail au Conseil de l'Europe. Dans le cadre de ces missions, il a pu rencontrer des agents à leur demande, s'entretenir avec les responsables de divers services, continuant d'entretenir ainsi un dialogue nourri et efficace avec les représentants de nombreuses entités administratives, ainsi qu'avec plusieurs agents impliqués dans le traitement de données à caractère personnel par l'Organisation. Il s'est également entretenu régulièrement avec le Comité du personnel et son président en relation avec des traitements de données relatifs aux agents. Il a également rencontré le Secrétaire général adjoint, ce fut l'occasion de faire un état de la situation en matière de protection des données au sein du Conseil de l'Europe.

Durant la période de référence aucune plainte formelle n'a été introduite auprès du Commissaire.[10] Des demandes, notamment concernant l'exercice du droit d'accès, lui ont été transmises, elles ont pu être traitées en premier ressort par la DPO. Il a également demandé des éclaircissements en rapport avec le déploiement de plusieurs outils informatiques et il a ouvert une enquête concernant l'introduction de Zoom au Conseil de l'Europe.

Le Commissaire a également publié des déclarations à l'occasion de la 17ème et de la 18ème édition de la journée de la protection des données et a répondu à plusieurs sollicitations de médias. Il a répondu également à des enquêtes dans le cadre de projets de recherche scientifique.

[10] Dates des visites de travail : 14 décembre 2022, 20-21 février 2023, 5-6 juin 2023, 9-10 octobre 2023, 12-13 février 2024 et 5-7 juin 2024.

Durant la période de référence, le Commissaire a continué d'échanger et de collaborer avec le Comité de la Convention 108, sa Présidente et le Bureau du Comité.

3.2 Participation à des évènements extérieurs

Le Commissaire est régulièrement sollicité afin de participer à des séminaires ou à des conférences, qu'il s'agisse de présenter le cadre interne à l'Organisation ou la modernisation de la Convention 108 (« Convention 108+ ») et les travaux du Comité de la Convention (protection des données et intelligence artificielle, identité numérique, reconnaissance faciale, etc.). Durant la période de référence, le Commissaire a participé et est intervenu notamment aux événements suivants :

- 30 juin 2023, Strasbourg, Forum « *Sport et Droits humains* » ;
- 24-25 October 2023, Interpol, Lyon: « *International Organisations Workshop on Data Protection*";
- 7 novembre 2023 Strasbourg, Séminaire sous l'égide du TACE relatif au règlement de la protection des données.

Le Commissaire n'a pas participé, notamment pour des questions budgétaires et organisationnelles, à la 45e Assemblée mondiale pour la protection de la vie privée (GPA) qui a eu lieu aux Bermudes de 15 à 20 octobre 2023. Il a toutefois suivi les travaux de la GPA tout au long de l'année et soutenu plusieurs résolutions adoptées lors de la 45e Assemblée mondiale.

4. Conseils et recommandations aux entités du Conseil de l'Europe

Le Commissaire a été appelé à émettre des avis ou des recommandations concernant le respect du droit à la protection des données personnelles à travers différents domaines d'activité ou différentes technologies. Les principaux sujets abordés sont résumés ci-dessous par service/entité concerné(e).

4.1 Direction des Services Généraux (DGS)

Divers sujets ont été abordés, notamment, la question de la vidéosurveillance, qui est toujours à l'ordre du jour de la Direction. Le Commissaire note avec satisfaction qu'une nouvelle signalétique conforme au nouveau règlement a été mise en place et qu'un document sur les bonnes pratiques en matière de vidéosurveillance va être adopté. Le Commissaire consulte régulièrement les registres d'extraction (vidéosurveillance et badges). Lors de sa dernière visite en février 2024, la Direction a informé le Commissaire de l'audit en cours de l'Etat-Hôte pour les bâtiments du Conseil à Strasbourg. Des discussions ont été également menées sur la mise en place d'un système d'accès au bureau par badge. En outre, les efforts particuliers sont poursuivis par la Direction conjointement avec la Direction des Technologies de l'Information (*DIT*), pour les bureaux du Conseil de l'Europe dans les pays-membres, avec pour objectif une mise à niveau conforme aux standards de Strasbourg.

À la suite des changements de *modus operandi* de l'Organisation après la pandémie COVID-19, le Commissaire et l'Administration ont mené un dialogue intense sur la corrélation entre la pratique accrue des réunions en ligne et la nécessité de garantir la protection des données personnelles. Il est intervenu à plusieurs reprises avec la DPO au sujet de l'utilisation de caméras dans les salles de réunion et a exigé l'établissement d'une analyse d'impact relative à la protection des données. Ces interventions ont permis d'opérer une claire distinction dans la gestion des caméras de sécurité présentes dans les salles de réunions et les systèmes de visio-conférence. Le Commissaire a rappelé les obligations en matière de transparence et exigé une meilleure information des personnes concernées sur l'utilisation des caméras. Une information devrait être disponible dans chaque salle de réunion. D'autres questions sont encore en cours d'examen et notamment l'utilisation du floutage, les processus de traitement des données, notamment la politique de suppression des données, le transfert de fichiers via le cloud, etc. En outre, une politique de l'audiovisuel englobant les exigences de protection des données devra être mise en place.

4.2 Direction des Ressources Humaines (DRH)

Plusieurs sujets sont à l'ordre du jour du dialogue régulier entre la DRH et le Commissaire. Notamment durant la période de référence, le Commissaire a émis des recommandations sur la gestion des dossiers du personnel, leur digitalisation et l'actualisation, la problématique de la transparence lors des concours internes, la procédure d'exercice du droit d'accès, ainsi que la question de la vérification (*vetting*) ou analyse de sécurité lors du recrutement qui sera introduite pour anticiper les risques réputationnels et de sécurité au sein de l'Organisation. Le recours à cette procédure de vérification doit être suivie de près du point de vue des garanties de la protection des données personnelles. Conformément aux principes de proportionnalité et de nécessité, le Commissaire recommande de définir les fonctions devant être soumises à cette procédure et de distinguer le niveau d'analyse eu égard aux risques encourus. Le degré d'analyse le plus invasif doit être réservé aux fonctions présentant un risque élevé.

Par ailleurs, les interlocuteurs ont abordé la question de l'utilisation de l'Intelligence Artificielle dans le processus de recrutement. Le Commissaire relève l'importance d'assurer la qualité des données traitées dans le système et également la nécessité du regard humain avant toute prise de décision.

Finalement, il faut noter que la DRH est ouverte à travailler conjointement avec le Commissaire et la DPO sur l'introduction d'une formation interne sur la protection des données personnelles pour tous les agents.

- ***Service médical***

Le Commissaire s'est également entretenu avec le service médical et a pu constater que toutes les données médicales sont traitées de manière strictement confidentielle. Un double système de stockage (papier et numérique) a été mis en place. Pour l'aspect numérique, le service a recouru à des logiciels spécifiques, sécurisés et cryptés, auxquels seules les deux médecins et les infirmières ont accès. Les dossiers « papiers » sont conservés sous clé. Les données médicales sont conservées 30 ans avant destruction. Les données ne sont pas transmises aux assurances.

4.3 Direction des Technologies de l'Information (DIT)

Le dialogue entre la DIT et le Commissaire est régulier, surtout s'agissant la sécurité des données[4]. Le Commissaire est notamment informé des activités récentes en matière de sécurisation des systèmes informatiques du Conseil de l'Europe afin de garantir la protection et la sécurité des données et parer les attaques de hackers.

La question des outils de stockage des médias-audiovisuels reste également parmi les priorités. Pour certains outils de stockage, la nomenclature n'est pas encore en place et nécessitera des analyses supplémentaires, en collaboration étroite avec la DIT (ex : pour la mise en place du processus de tableau de gestion, sur la politique de suppression de données, etc.…). De manière générale, toute la politique de stockage des données personnelles et leur durée de conservation doit être revue. Le Commissaire privilégie le stockage des données, au moins pour les données sensibles, sur des supports internes à l'organisation. Le recours à l'info-nuage, s'il s'avère nécessaire, doit répondre à des exigences élevées de sécurité et en particulier au chiffrement des données.

Le Commissaire et la DPO suivent de près les discussions menées par DIT au sein de l'Organisation sur l'introduction de l'Intelligence Artificielle. Notamment la question se pose pour l'utilisation de l'IA pour l'évaluation et la réévaluation des données déjà collectées.

L'introduction de Zoom au début 2023, dont le Commissaire n'avait pas été préalablement informé, a fait l'objet d'une procédure d'examen minutieuse. Sur la base d'un rapport circonstancié de l'Unité

[4] *Voir également point 6 « Sécurité des données » ci-dessous*.

de protection des données établi à sa demande, le Commissaire a adressé à l'administration une série de questions afin de s'assurer que le recours à Zoom se ferait dans le respect des dispositions du règlement de protection des données. La procédure a nécessité plusieurs séances de clarification et plusieurs relances du Commissaire pour obtenir les réponses aux différentes questions. Elle a débouché sur deux recommandations formelles.

Dans ses conclusions et d'un point de vue de la protection des données, le Commissaire estime qu'il n'y a pas lieu de remettre en cause le recours à Zoom. Il attend néanmoins que ses recommandations soient prises en considération. La conduite de ce dossier s'est heurtée à une certaine incompréhension, voire sous-estimation de l'administration, du rôle, statut et fonctions du Commissaire, ce qui n'a pas facilité l'obtention des réponses aux questions du Commissaire. Un certain flou a également été constaté dans la collaboration entre les différents services impliqués.

Ce dossier met également l'accent sur le poids des grandes entreprises du numérique qui veulent imposer de manière unilatérale leurs conditions générales et leurs contrats d'utilisation sans tenir compte des particularités d'une Organisation internationale comme le Conseil de l'Europe. L'intervention du Commissaire a permis néanmoins que Zoom accepte la référence aux clauses contractuelles types adoptées par le Comité 108 et au règlement de protection des données du CoE. Le Commissaire invite les Organisations internationales à examiner la possibilité de se regrouper pour négocier avec les entreprises du numérique eu égard aux exigences de protection des données.

4.4 Direction de l'Audit Interne et de l'Evaluation

Durant la période de référence, le Commissaire et la Direction de l'Audit interne et de l'évaluation ont abordé plusieurs questions. Un audit sur le recrutement interne a notamment eu lieu en 2023 et les questions des données personnelles se sont posées. Ceci a permis d'alimenter les conclusions et les recommandations adressée à la DRH. Ainsi, l'Audit interne inclut désormais la protection des données personnelles dans leur ligne d'évaluation des risques.

Un audit sur le management des missions/voyages aura lieu vers la fin de l'année 2024 et la problématique de la protection des données personnelles sera prise en compte lors d'évaluation du système GDD.

Finalement, un audit de la mise en œuvre du nouveau Règlement de protection des données pourrait être mené à la fin de la période transitoire et à ce titre des échanges réguliers entre le Commissaire et la Direction de l'Audit Interne et de l'Evaluation sont nécessaires.

4.5 Tribunal administratif (TACE)

Le Commissaire a également eu des contacts avec le greffe du Tribunal administratif qui ont permis d'expliquer le rôle du Commissaire en relation avec le TACE, d'aborder différentes problématiques liées à l'anonymisation des données et de la confidentialité des données lors de l'utilisation du courriel. Le Commissaire a rappelé la nécessité de recourir à un système de messagerie sécurisé.

5. Déléguée à la protection des données (DPO)

Comme indiqué précédemment, le nouveau Règlement prévoit à l'Article 13 la mise en place au minimum d'un(e) délégué(e) à la protection des données qui doit être impliqué(e) dans toutes les questions relatives à la protection des données. La désignation est faite sur la base de leurs qualités professionnelles, de leur capacité à remplir les tâches visées au Règlement et, en particulier, de leurs connaissances spécialisées des normes et pratiques en matière de protection des données.

Il convient de souligner que grâce à l'arrivée de la DPO, la protection des données des agents et personnes interagissant avec le Conseil de l'Europe a progressé et commence – bien que lentement - à être intégrée par les différents services de l'Organisation.

Néanmoins, à l'heure actuelle une seule DPO est désignée au sein de l'Organisation. En conformité avec le nouveau Règlement, elle traite les dossiers applicables à tous les membres du Secrétariat du Conseil de l'Europe (agents, détachés, stagiaires) ainsi qu'aux interlocuteurs extérieurs (experts, consultants, participants aux événements du Conseil de l'Europe, visiteurs) dont les données personnelles sont traitées par le Conseil de l'Europe. Ces tâches sont déjà considérables pour une personne et la collaboration interne n'est pas toujours aisée. A noter également que la question de la cartographie des données devient urgente pour l'Organisation et en absence d'outil au Conseil de l'Europe pour gérer ces données, la tâche est également insurmontable pour une seule personne.

Durant la période de référence, le Commissaire a travaillé conjointement avec la DPO sur divers sujets (adoption du nouveau Règlement sur la protection des données, les besoins de l'outil pour la cartographie des données, les différentes politiques de confidentialité, notamment celles relatives aux réunions utilisant les caméras et les systèmes de visioconférence, les demandes d'accès par les ex-employés du Conseil de l'Europe à leurs données personnelles, etc.). A sa demande, le Commissaire lui donne également son avis sur différents projets et analyses d'impact relative à la protection des données. Les échanges sont réguliers sur ces différents sujets.

En outre, en 2024, le Commissaire et la DPO, avec un soutien de l'Unité de protection des données et l'Unité HELP (DG-1), ont travaillé conjointement sur le contenu de la formation interne destinée aux agents du Conseil de l'Europe et visant à leur sensibilisation aux exigences en matière de protection des données. Ce travail visant la formation en ligne, obligatoire pour tous les agents de l'Organisation, est toujours en cours d'élaboration et est prioritaire.

6. Sécurité des données

La sécurité des données est inscrite à l'article 6 « sécurité des données » du nouveau Règlement du Conseil de l'Europe sur la protection des données à caractère personnel. L'article 6.5 prévoit l'obligation de la Déléguée à la protection des données d'informer le Commissaire en cas de violations de données. Le Commissaire a néanmoins rappelé que les violations de données doivent être annoncées sans délai indépendamment d'une information à la Secrétaire générale.

Durant la période écoulée, plusieurs failles de sécurité ou violations de protection des données ont été signalées au Commissaire. A chaque incident, les services concernés ont fait preuve d'une grande réactivité et les services concernés ont pris les mesures nécessaires, en coordination avec la Direction des technologies de l'information et la DPO.

Une action prioritaire doit être menée par l'Organisation pour soutenir la DIT, la DPO et le Commissaire dans leurs efforts visant la sécurité des données. Ceci est d'autant plus important à la lumière de nouveaux dossiers sensibles de l'Organisation (en particulier le fonctionnement du nouveau Registre des dommages pour l'Ukraine, la volonté de l'Organisation de consolider sa coopération avec certaines forces démocratiques et représentants de la société civile en exile, etc.).

7. Conclusions

Avec l'adoption de son nouveau Règlement de protection des données, une nouvelle ère s'ouvre pour le Conseil de l'Europe. L'entrée en vigueur de ce règlement constitue une étape importante pour garantir le respect des droits humains et des libertés fondamentales, notamment le droit à la vie privée des personnes lors du traitement de données personnelles au sein de l'Organisation.

Le texte réglementaire ne suffit pas, cependant, à assurer la protection des données. L'Administration a déjà entamé le processus de mise en conformité avec le Règlement. Un accent prioritaire doit cependant être mis sur la formation et la sensibilisation afin que les différents services et agents intègrent la protection des données au quotidien. Après plus d'une année d'entrée en vigueur, par exemple, trop souvent encore les analyses d'impact en matière de protection des données ne sont menées que pour donner suite à l'intervention du Commissaire ou de la DPO.

Il convient aussi d'allouer rapidement les ressources humaines, financières, matérielles et techniques en particulier à la DPO et au Commissaire, lesquelles sont indispensables pour assurer l'effectivité de la protection des données au sein de l'Organisation. Ce n'est hélas actuellement pas le cas. A l'heure actuelle, la DPO est submergée et ne peut accomplir l'ensemble de ses tâches. Quant au Commissaire qui œuvre à titre bénévole, il ne peut compter que sur un soutien limité de l'Unité de protection des données, laquelle ne dispose déjà pas des ressources humaines et financières suffisantes pour les tâches qui lui incombent, sans compter les activités d'évaluation prévues dans la Convention 108+. Il n'est ainsi pas en mesure d'approfondir autant qu'il se devrait les questions pointues auxquelles il doit faire face, ni de procéder à des contrôles effectifs du respect des dispositions de protection des données.

Conformément à la Convention 108+ et au Règlement, le/la Secrétariat Général(e) se doit d'accorder au Commissaire les ressources nécessaires à l'accomplissement effectif de ses fonctions et à l'exercice de ses pouvoirs. Sans ressources adéquates et la volonté politique de donner une place prioritaire à la protection des données personnelles au sein du Conseil de l'Europe, le Règlement risque de demeurer lettre morte portant notamment atteinte à la crédibilité de l'Organisation.