



Strasbourg, 20 avril 2022

T-PD-BUR(2022)1

**BUREAU DU COMITE CONSULTATIF DE LA CONVENTION
POUR LA PROTECTION DES PERSONNES A L'EGARD DU
TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL**

CONVENTION 108

**Avis sur le projet de Résolution instituant le Règlement du Conseil de l'Europe sur la
protection des données à caractère personnel**

I. Introduction

1. Par courrier du 16 mars adressé à la présidente du T-PD, le directeur de la Direction générale de l'administration (DGA), tenant compte des demandes de consultation maintes fois formulées par le T-PD, a sollicité l'avis du bureau du comité consultatif au sujet du projet de résolution instituant le Règlement du Conseil de l'Europe sur la protection des données à caractère personnel. L'avis devrait être adopté d'ici au 20 avril pour permettre la saisine du Comité des Ministres en mai 2022 et une entrée en vigueur le 1^{er} juillet 2022. L'avis du bureau doit porter principalement sur la conformité du projet de règlement avec les dispositions de la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+).
2. A titre préliminaire, il convient de s'interroger sur la question de savoir si le bureau est compétent pour adopter un avis de conformité à la Convention 108+ ou si cette compétence n'est pas du ressort du T-PD. Aux termes de l'article 10bis §3 du règlement intérieur du T-PD, le bureau élabore et approuve les avis demandés par des organes du Conseil de l'Europe. Il est dès lors a priori compétent pour adopter un avis conformément à la demande de la DGA. Aux termes de l'article 10bis § 4, il devrait néanmoins consulter le comité avant d'adopter son avis. L'adoption de l'avis intervient par consensus. En cas de désaccord, il revient au comité de trancher. Vu la nature et l'objet de l'avis demandé et vu l'article 23, lettre f de la Convention 108+ (examen de conformité), le bureau estime néanmoins qu'il eut été préférable que l'avis soit formellement adopté par le comité plénier.
3. Tenant compte du court délai qu'il lui a été accordé, malgré le fait que le processus d'élaboration du nouveau règlement a pris plusieurs années et qu'il eut été parfaitement envisageable de consulter le T-PD dans des délais raisonnables lui permettant d'adopter un avis de conformité lors d'une plénière régulière, le bureau, , a adopté, par procédure écrite, l'avis suivant :

II. Appréciation générale

4. Le projet de règlement du Conseil de l'Europe sur la protection des données à caractère personnel doit remplacer le règlement du Secrétaire général du 17 avril 1989 instaurant un système de protection des données pour les fichiers de données à caractère personnel. Ce règlement est obsolète et ne répond plus aux exigences actuelles de protection des données de la Convention 108 et de la Convention 108+. Le Comité consultatif avait d'ailleurs invité dès les années 2010 et à plusieurs reprises le Secrétariat général du Conseil de l'Europe à élaborer un nouveau règlement qui soit en ligne avec les dispositions de la Convention.
5. Le bureau reconnaît et salue la volonté du Secrétariat général de se doter d'une réglementation moderne et conforme aux dispositions de la Convention 108+ afin d'assurer un niveau de protection des données robuste au niveau de l'Organisation.

6. Après examen du projet qui lui a été soumis, le bureau, sous réserve des quelques remarques et propositions ci-dessous, parvient à la conclusion que **le projet de règlement répond et est conforme aux exigences de la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+)**.
7. Le projet de règlement suit, autant que relevant, la structure de la Convention 108+ et comprend trois sections, à savoir Dispositions générales (objet et but, définitions, champ d'application), Principes pour la protection des données à caractère personnel (légitimité du traitement et qualité des données, données sensibles, sécurité des données, transparence du traitement, droits des personnes concernées, obligations complémentaires, restrictions, transfert de données en dehors de l'organisation), Autorités consultatives et de contrôle¹.

III. Remarques et propositions

Projet de résolution

Dans le préambule, il conviendrait au dernier paragraphe de mentionner que le bureau du T-PD a été consulté.

Projet de règlement

Section I – Dispositions générales

Article 2 – Définitions

Dans la version française, nous proposons de reprendre la terminologie de la Convention 108+ pour l'article 2.5, à savoir « ... qui reçoit communication de données ou à qui des données sont rendues accessibles »

Section II – Principes pour la protection des données à caractère personnel

Article 4 – Légitimité du traitement de données et qualité des données

Nous suggérons de revoir la rédaction du 4.2.1 et d'éviter le point-virgule entre États membres et l'exercice d'autres activités.

A l'article 4.2.3, même si cela ressort de la définition du consentement, nous proposons d'ajouter après personne concernée « ou de son représentant légal » pour éviter toute ambiguïté.

A l'article 4.3.2, nous proposons de rajouter « complémentaires » après « sous réserve de garanties appropriées » (voir article 5.4.b Convention 108+ et article 5.1 du Règlement du Conseil de l'Europe sur la protection des données à caractère personnel). En effet si les garanties doivent effectivement être appropriées, elles viennent compléter et non pas se substituer aux autres garanties du règlement.

¹ Dans la version française, il convient de remplacer chapitre III par Section III.

Article 4.2.6 : il est proposé de biffer ce paragraphe étant donné qu'un tel motif justificatif n'est prévu qu'essentiellement pour des responsables du traitement du secteur privé. Il convient de noter que le RGPD exclut la possibilité de recours à l'intérêt légitime des organismes publics dans l'accomplissement de leurs fonctions (article 6.1.f) et que le Règlement (UE) 2018/1725 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions de l'UE n'inclut pas l'intérêt légitime dans son article 5.

Article 6 – Sécurité des données

Il est proposé d'ajouter après responsable du traitement « ainsi que, le cas échéant, le sous-traitant » pour répondre à l'exigence de l'article 7.1 de la Convention 108+ également au sous-traitant de prendre les mesures de sécurité appropriées.

Article 7 – Transparence du traitement de données

A l'article 7.1.1, il serait souhaitable d'ajouter « de son identité » avant « ses coordonnées ». Il serait également souhaitable d'ajouter les coordonnées du Délégué à la protection des données ainsi que du Commissaire à la protection des données en tant qu'autorités de protection des données compétentes. Cela garantirait une accessibilité des personnes concernées à un mécanisme de contrôle et de recours effectif.

A l'article 7.2 in fine, nous nous interrogeons sur le fait de savoir si l'exception « est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement » a une raison d'être et le cas échéant si elle ne doit pas être déplacée à l'article 10 pour autant que cette exception ne soit pas déjà suffisamment reflétée dans les motifs de restrictions qui y sont énoncées. Alternativement, ce passage pourrait être remplacé par « dès lors que le traitement est expressément prévu par la loi ». Ceci correspondrait à l'art. 8, para 3 de la Convention 108+. Si cette disposition est conservée, on pourrait y ajouter : « Dans ce cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés fondamentales, ainsi que les intérêts légitimes de la personne concernée. »

Article 8 – Droits des personnes concernées

Nous proposons de rajouter le droit de bénéficier de l'assistance de l'autorité de contrôle, à savoir du Commissaire. L'article 9.1.e de la Convention 108+ prévoit que toute demande de rectification ou d'effacement soit sans frais, nous suggérons donc d'ajouter dans l'article 8.4 « sans frais » après « d'obtenir à sa demande... ».

Article 9 – Obligations complémentaires

Aux articles 9.2 et 9.3, il est proposé d'ajouter après responsable du traitement « ainsi que, le cas échéant, le sous-traitant » afin de prévoir les mêmes obligations pour les sous-traitants, conformément à l'article 10, points 1 et 2, de la Convention 108+.

A l'article 9.5, la compétence de prévoir des mesures appropriées ne relève-t-elle pas plutôt du responsable de traitement que de l'Organisation ?

A l'article 9.6, le fait de confier le traitement des données à un sous-traitant ne doit pas délivrer le responsable du traitement de sa responsabilité. Le libellé retenu prête à confusion et nous proposons de remplacer « n'attribue la responsabilité du traitement... » par « n'attribue l'exécution du traitement de données à caractère personnel à un sous-traitant ».

Article 10 – Restrictions

Il est proposé de rajouter « complémentaires » sous garanties appropriées.

Article 12 – Transfert de données à caractère personnel en dehors de l'Organisation

Le constat du niveau de protection équivalent (art. 12.1) est un travail complexe. Il serait probablement plus approprié de confier cette tâche à l'Organisation après consultation obligatoire du Commissaire voire du Comité conventionnel. Rappelons que dans l'UE, conformément au RGPD, c'est la Commission européenne qui décide du niveau d'adéquation d'un État ou d'une organisation internationale, mais seulement après consultation du Comité Européen de la Protection des Données et du Parlement Européen, et avec le consentement des Etats-membres.

A l'article 12.3.2 in fine, le passage « ou lorsqu'elle est physiquement ou juridiquement incapable de donner son consentement » est en contradiction avec la définition du consentement de la personne concernée qui intègre le consentement du représentant légal.

Section III – Autorités consultatives et de contrôle

Article 13 – Délégué(s) à la protection des données

Nous saluons l'instauration d'un – ou de plusieurs – délégué(s) à la protection des données au sein de l'Organisation. La Convention 108+, qui énonce les principes à suivre sans donner les détails pour leur application, ne comprend pas formellement une telle exigence. Cependant, la mise en œuvre des dispositions contraignantes qu'elle contient implique au moins qu'une organisation de protection des données soit mise en place pour assurer la mise en conformité et la démonstration de la conformité. La nomination d'un délégué (DPO) est une bonne option. Le DPO est ainsi un maillon central de l'exigence de conformité de l'article 10.1 de la Convention 108+.

Le DPO doit pouvoir bénéficier d'une certaine indépendance dans l'exercice de ses fonctions, ce qui d'ailleurs est bien reflété à l'article 13. L'article 13 ne dit rien par contre par rapport au rattachement du DPO. Or il est important que celui-ci/ceux-ci ne soi(en)t pas rattaché(s) à une direction qui peut être exposée du point de vue de la protection des données, notamment qui traite les données du personnel de l'Organisation, qui est en charge des systèmes d'information ou qui est en charge de la sécurité ou de l'évaluation des risques.

Il pourrait être ajouté au paragraphe 13.4.2 après « de manière indépendante »: « - notamment par rapport au responsable du traitement ainsi que de la direction concernée - ».

Avec la nouvelle réglementation et conformément à la Convention 108+, la mise en œuvre de la protection des données incombera principalement aux différentes instances et agents du Conseil de l'Europe qui traitent des données à caractère personnel (obligation de conformité et de démonstration) et au DPO, lequel doit veiller à la bonne application des dispositions. Le DPO, nommé par le Secrétaire Général, est l'organe interne responsable d'assurer la protection des données au sein de l'organisation. Il soutient et conseille les différents services, traite principalement les demandes des personnes concernées et sensibilise l'organisation à la protection des données. Il est le point de contact et collabore avec l'autorité de contrôle « externe », le Commissaire à la protection des données.

Articles 15ss Commissaire à la protection des données

Les articles 15 à 17 du nouveau règlement régissent le Commissaire à la protection des données du Conseil de l'Europe comme autorité de contrôle de l'Organisation. Ses fonctions et ses tâches découlent du régime renforcé défini dans les chapitres IV et V de la Convention 108+, qui sont consacrés aux autorités de contrôle, et plus particulièrement les articles 15 et 17.

En tant qu'autorité de surveillance, conformément à la Convention 108+, le Commissaire devrait :

- agir de manière indépendante et impartiale dans l'accomplissement de ses tâches et l'exercice de ses pouvoirs, sans solliciter ni accepter d'instructions de quiconque ;
- disposer des ressources nécessaires à l'accomplissement efficace de ses fonctions et à l'exercice de ses pouvoirs ;
- disposer de pouvoirs d'investigation et d'intervention ;
- être compétent dans le domaine des flux transfrontaliers de données pour approuver des clauses juridiques standardisées ;
- être en mesure de prendre des décisions sur les violations des dispositions de la Convention et notamment de sanctionner les infractions administratives (pouvoirs autonomes de décision et de sanction) ;
- pouvoir intenter des actions en justice ;
- être responsable de la sensibilisation et de l'éducation du public en matière de protection des données ;
- être consulté sur toute proposition législative ou administrative impliquant le traitement de données à caractère personnel.

Pour renforcer et souligner l'indépendance structurelle du Commissaire à la protection des données, nous proposons les changements suivants à l'article 15:

- 15.6 Le Commissaire à la protection des données devra être doté des ressources humaines, techniques et financières, des locaux et de l'infrastructure nécessaires à l'exécution efficace de ses tâches par l'Organisation conformément aux modalités établies par le Comité des Ministres qui consacrera un budget annuel fixe distinct au Commissaire à la protection des données.

15.7 Le Commissaire à la protection des données bénéficie d'un secrétariat adéquat nécessaire à l'exercice efficace de ses fonctions et à l'exercice de ses pouvoirs. Il choisit son propre personnel qui est placé sous sa direction exclusive.

Un élément important est le rôle de sensibilisation et d'éducation à la protection des données. Cela concerne le public, qui doit être sensibilisé aux risques, cachés ou non, découlant des évolutions techniques et sociétales. Selon le rapport explicatif de la Convention (également adopté par le CM au moment de l'adoption et de l'ouverture de la signature de la Convention modernisée), « [...] *l'autorité de contrôle assure de manière proactive la visibilité de ses activités, fonctions et pouvoirs.* » A cette fin, l'autorité de contrôle doit « *informer le public par des rapports périodiques [...]* ». Elle peut « *également publier des avis, émettre des recommandations générales relatives à la bonne application des règles de protection des données ou utiliser tout autre moyen de communication. Par ailleurs, elle doit fournir des informations aux individus et aux responsables du traitement ainsi qu'aux sous-traitants sur leurs droits et obligations en matière de protection des données. Dans leur travail de sensibilisation aux questions relatives à la protection des données, les autorités de contrôle devront veiller à s'adresser spécifiquement aux enfants et aux catégories de personnes vulnérables par des moyens et des langues adaptés* »².

Le Commissaire ne se limite plus à veiller à l'application des normes au sein de l'organisation, il doit pouvoir s'exprimer sur les grandes questions que soulève le respect du droit à la protection des données. A cet égard, les autorités de contrôle doivent être en mesure d'anticiper les risques potentiels dus au développement des technologies de l'information et de la communication ("veille technologique") et d'alerter le public et le Conseil de l'Europe sur ces risques. Cette fonction de sensibilisation est fondamentale, notamment pour permettre aux individus de mieux garder le contrôle sur leurs données et d'exercer leurs droits. L'exercice de cette mission nécessite une présence extérieure et une visibilité du Commissaire qui ne peut se limiter à la publication de son rapport d'activités.

De manière tout à fait satisfaisante, le projet de règlement énumère les fonctions et les pouvoirs du Commissaire conformément à la Convention. Il a toutefois passé sous silence les tâches de sensibilisation et l'obligation de consulter le Commissaire sur les propositions législatives ou administratives impliquant des traitements de données à caractère personnel. Ces deux tâches doivent être insérées dans le projet de règlement.

Une autre fonction essentielle du Commissaire est la coopération avec les autorités nationales et internationales de protection des données. Cette tâche est incluse dans le projet de règlement. En vertu de la Convention 108+, il s'agit d'une obligation. Dans un contexte mondial et interconnecté, l'efficacité de la protection des données exige une telle coopération. Ce rôle externe du Commissaire est crucial et doit être souligné : il s'agit avant tout de coopération internationale, c'est-à-dire avec toute autre autorité de contrôle de la protection des données. Il s'agit également de la sensibilisation, de la formation, de l'échange de personnel ou du partage d'informations. En revanche, il n'incombera pas aux Commissaires de s'immiscer dans les compétences d'évaluation du Comité conventionnel, ni d'intervenir dans les compétences des autorités de protection des données des Parties ou de porter un jugement sur la manière dont les Parties remplissent leurs obligations.

² Rapport explicatif, § 125.

Article 18 Réclamations et recours

Cette disposition règle la procédure en cas d'une réclamation adressée au Commissaire. Elle prévoit une voie de droit contre les décisions du Secrétaire Général prises conformément aux conclusions du Commissaire. Cette voie de droit est différente s'il s'agit de membres du personnel ou d'anciens membres du personnel ou s'il s'agit de personnes externes à l'Organisation. Dans le premier cas, la voie de droit est le Tribunal administratif du Conseil de l'Europe. Dans le second et en l'absence d'accord à l'amiable, le litige sera réglé par un arbitrage conformément au Règlement facultatif d'arbitrage entre les organisations internationales et les parties privées de la Cour permanente d'arbitrage à la Haye. Un recours effectif est fondamental à garantir la protection des données personnelles et de la vie privée. On est donc en droit de s'interroger si cette différence se justifie et si elle n'est pas propre à décourager les personnes externes à faire valoir leurs droits par le biais de l'arbitrage. Le bureau invite le Secrétariat général à reconsidérer la question et à examiner la possibilité de confier au Tribunal administratif ou à un juge de la CEDH le soin de traiter un recours émanant d'une personne externe à l'Organisation. Si cela s'avère impossible en raison de la structure juridique des tribunaux, il faudrait au moins s'assurer que le coût de l'arbitrage est en général – avec des exceptions raisonnables comme des plaintes excessives et répétitives – supporté par l'Organisation. Les coûts (élevés) de l'arbitrage pourraient avoir un effet dissuasif autrement. En ce qui concerne l'arbitre, il serait recommandé de s'assurer qu'il possède l'expérience pertinente en matière de droit de la protection des données.

IV Conclusion

Le Bureau du T-PD salue l'adoption de ce nouveau règlement et soutient son adoption en vue d'une entrée en vigueur rapide. Toutefois, il invite le Secrétariat général à tenir compte des remarques et propositions formulées ci-dessus et d'adapter le projet en conséquence. Au cas où le Secrétariat général s'écarte du présent avis, il l'invite à porter son avis à la connaissance du CM lors de la transmission du projet de règlement.