COUNCIL OF EUROPE DEVELOPMENT BANK
BANQUE DE DEVELOPPEMENT DU CONSEIL DE L'EUROPE

Rapport annuel du Commissaire à la protection des données

1er octobre 2022 - 31 décembre 2023

RAPPORT ANNUEL DU COMMISSAIRE À LA PROTECTION DES DONNÉES 2023

(traduit de l'original en anglais)

Contenu

Billy Hawkes

Janvier 2024

Résumé

Il s'agit de mon premier rapport en tant que Commissaire à la protection des données. Il couvre la période allant de ma nomination le 1er octobre 2022 au 31 décembre 2023. Au cours de cette période de 15 mois, j'ai principalement travaillé avec le Délégué à la protection des données (DPO) afin d'assurer la pleine conformité avec les exigences du Règlement à l'expiration de la période de transition pour la mise en œuvre, le 1er juillet 2024. J'estime que la Banque respecte pour l'essentiel les normes élevées qu'elle s'est fixées dans les règlements révisés. Mes conclusions sur la seule plainte substantielle que j'ai traitée n'ont révélé aucun élément de non-conformité, sur la base d'un examen rigoureux de tous les aspects du traitement par la Banque des données relatives au personnel, la principale catégorie de données à caractère personnel traitées par la Banque. À l'avenir, la Banque est bien placée pour pouvoir démontrer, en tant que membre de la famille du Conseil de l'Europe, qu'elle continuera à respecter les normes élevées que l'on attend d'elle dans un domaine où le Conseil a joué un rôle majeur de normalisation.

Introduction

1. Il s'agit de mon premier rapport en tant que Commissaire à la protection des données. Il couvre la période allant de ma nomination, le 1er octobre 2022, au 31 décembre 2023. Il est établi conformément à l'article 17 du règlement relatif à la protection des données de la CEB, qui dispose que le Commissaire *établit un rapport annuel décrivant ses activités. Ce rapport est transmis au Gouverneur et rendu public*.
2. Au cours de cette période de 15 mois, j'ai principalement travaillé avec le Délégué à la protection des données (DPO) pour veiller à ce que les exigences du règlement soient pleinement respectées.
3. J'ai visité le siège de la Banque à Paris à huit reprises. Au cours de ces visites, j'ai rencontré le Gouverneur de la Banque ainsi que des directeurs et des cadres supérieurs. Tous m'ont assuré de leur engagement à ce que la Banque respecte les normes élevées de protection des données énoncées dans son Règlement sur la protection des données, qui reflète à son tour le rôle de premier plan joué par le Conseil de l'Europe dans la promotion des normes les plus élevées dans ce domaine. J'ai également eu une réunion (sur Zoom) avec le Comité du personnel et j'ai participé à une réunion des parties prenantes avec le Tribunal administratif.

Règlement de la CEB sur la Protection des données

4. Le Règlement est entré en vigueur le 1er juillet 2022, après son approbation par le Conseil d'administration. L'article 20 prévoit une période de transition de deux ans pour mettre les activités de traitement en conformité avec le règlement. Le Règlement a remplacé un système antérieur de protection des données entré en vigueur en 2008.
5. Le Règlement prévoit un système complet de protection des données à caractère personnel au sein de la Banque, qui s'inspire étroitement des dispositions de la *Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel* ("Convention 108+") et du *Règlement du Conseil de l'Europe sur la protection des données à caractère personnel*. Elles impliquent un renforcement des dispositions de gouvernance en matière de protection des données, notamment par le remplacement d'un comité interne par un commissaire externe indépendant.
6. La responsabilité de la conformité incombe aux *responsables du traitement des données*. Le *responsable du traitement* est défini à l'article 2 comme *toute entité administrative, organe, institution ou autorité au sein de la Banque qui, seul ou conjointement avec d'autres, a le pouvoir de décision en ce qui concerne le traitement des données, que ce pouvoir découle d'une désignation légale ou de circonstances de fait*.

Rôle du Commissaire

7. Les articles 15 et 16 prévoient la nomination et les fonctions du Commissaire (DPC). L'article 15.3 stipule que le Commissaire *agit en toute indépendance et impartialité dans l'exercice de ses fonctions et de ses pouvoirs en vertu du présent règlement et, ce faisant, ne sollicite ni n'accepte d'instructions*. L'article 16 stipule que le Commissaire a les fonctions suivantes :
   a) contrôler et assurer l'application des dispositions du présent Règlement ;
   b) examiner les réclamations des personnes concernées concernant une violation alléguée de leurs droits en vertu du présent Règlement et d'ordonner des mesures correctives si nécessaire ;

c) *effectuer des enquêtes sur l'application du présent Règlement, soit de sa propre initiative, soit pour examiner une réclamation d'une personne concernée ;*
d) *formuler des avis à la demande du/de la délégué(e) à la protection des données ou d'un/une responsable du traitement sur toute question relative à la mise en œuvre du présent Règlement ;*
e) *faire des recommandations à un/une responsable de traitement qui rendra compte ensuite au/à la Commissaire de leur mise en œuvre ;*
f) *coopérer avec les autorités nationales ou internationales de protection des données ou avec les autorités de protection des données d'organisations internationales dans la mesure nécessaire à l'exercice de ses missions et de ses pouvoirs.*

8. Le règlement confère au Commissaire des pouvoirs étendus d'enquête et d'exécution en ce qui concerne les données à caractère personnel traitées par la Banque.

Rôle du Délégué à la protection des données

9. Les articles 13 et 14 prévoient la nomination et les fonctions d'un *Délégué à la protection des données* (DPO). Au cours de la période couverte par le présent rapport, le DPO nommé par le Gouverneur était Nicolas BOUGOT, qui cumulait la fonction de DPO avec son rôle de Responsable de la Sécurité des Systèmes d'Information (RSSI). Je suis convaincu que ce cumul de fonctions répond aux exigences de l'article 13.2, selon lequel *les autres tâches professionnelles du Délégué à la protection des données doivent être compatibles avec ses fonctions de Délégué à la protection des données et ne doivent pas donner lieu à un conflit d'intérêts.* M. Bougot est titulaire d'une qualification professionnelle en matière de protection des données, délivrée par l'université de Maastricht.
10. Le DPO apporte son soutien et ses conseils aux responsables du traitement des données et aux personnes concernées afin de garantir une mise en œuvre correcte des règlements. Le DPO est également le principal point de contact du Commissaire à la protection des données.

Catégories de données à caractère personnel

11. L'article 9.8 du Règlement impose à chaque responsable du traitement l'obligation de tenir un registre des activités de traitement sous sa responsabilité contenant les informations suivantes :
a) *le nom et les coordonnées du/de la responsable du traitement et, le cas échéant, du sous-traitant et du/de la responsable conjoint du traitement ;*
b) *les finalités du traitement ;*
c) *une description des catégories de personnes concernées et des catégories de données à caractère personnel ;*
d) *les catégories de destinataires auxquelles les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans les États membres, les pays tiers ou les organisations internationales ;*
e) *le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées ;*
f) *dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;*
g) *dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 6, paragraphe 1.*

12. En prévision de l'entrée en vigueur du nouveau règlement, le DPO, avec l'aide d'un consultant, avait établi un relevé détaillé des activités de traitement (ROPA) décrivant les différentes catégories de données traitées par la Banque. Le DPO a pris des dispositions pour mettre à jour le ROPA, qui constitue désormais un registre complet des données à caractère personnel traitées par la Banque, qui doit être revu et mis à jour régulièrement. L'article 9. 8 (f), traite d'un aspect qui nécessite des travaux supplémentaires : *les délais envisagés pour l'effacement des différentes catégories de données.*
13. Le ROPA montre que la principale catégorie de données à caractère personnel traitées par la Banque est celle des données de ses employés et de ses prestataires. Il peut s'agir de *catégories particulières de données* telles que définies à l'article 5, comme les données à caractère personnel relatives à la santé et aux procédures disciplinaires. D'autres catégories comprennent les coordonnées de personnes au sein d'entités avec lesquelles la Banque traite en tant qu'emprunteur et prêteur de

fonds. La nature des activités de la Banque n'exige pas la collecte de données à caractère personnel des bénéficiaires finaux de ses prêts.

14. La Banque fait appel à un certain nombre d'agences externes pour effectuer des tâches spécialisées telles que la fourniture de services de paie. Chacun de ces arrangements fait l'objet d'un contrat, comme l'exige l'article 9.7. Le DPO a procédé à un examen de ces contrats et, dans un petit nombre de cas, certaines améliorations peuvent être souhaitables au moment du renouvellement des contrats.

Transparence

15. L'article 7 du règlement prévoit que le responsable du traitement *informe la personne concernée, si celle-ci n'est pas déjà informée, de ce qui suit :*
    a) ses coordonnées ;
    b) la base juridique et les finalités du traitement envisage ;
    c) les catégories de données à caractère personnel traitées ;
    d) les destinataires ou les catégories de destinataires des données à caractère personnel, le cas échéant ;
    e) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
    f) l'existence du droit de retirer son consentement à tout moment, lorsque le traitement est fondé sur le consentement de la personne concernée, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci; 5
    g) l'existence de toute décision automatisée, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée; et
    h) les moyens d'exercer ses droits énoncés à l'article 8 ci-dessous, ainsi que toute information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel.
16. Une note détaillée a été diffusée à l'ensemble du personnel de la Banque le 27 novembre 2023, donnant les informations suivantes énumérés ci-dessus, y compris les rôles du DPO et du DPC. La note est également disponible sur l'intranet de la Banque.

Promotion de la sensibilisation

17. L'article 14.2 (j), du règlement prévoit que l'une des tâches du *DPO consiste à sensibiliser la Banque aux principes de la protection des données, tels que les droits des personnes concernées et les obligations en matière de traitement des données à caractère personnel*. L'intranet de la Banque comporte une page consacrée à la protection des données, qui comprend des guides et une vidéo sur le sujet. Le DPO a dispensé une formation ciblée au personnel chargé des données relatives aux ressources humaines, la principale catégorie de données à caractère personnel traitées par la Banque. Il a également fourni des conseils détaillés sur la sécurité des données et sur l'utilisation des outils d'intelligence artificielle par le personnel de la banque.

Évaluations de l'impact sur la protection des données (DPIA)

18. L'article 9.4, du règlement oblige les responsables du traitement à consulter le DPO *lorsqu'un type de traitement de données à caractère personnel est susceptible de présenter un risque pour les droits et libertés fondamentaux des personnes concernées, en raison notamment de la nature et du volume des données ou de la nature, de la portée et de la finalité du traitement*, et le DPD doit consulter le CPD dans les cas appropriés. Le DPD s'est fortement impliqué en conseillant les responsables du traitement dans la préparation de ces AIPD et m'a consulté sur deux cas de ce type concernant le recours à des agences externes pour, respectivement, traiter les données relatives aux salaires et faciliter les performances du personnel.

Sécurité des données

19. L'article 6 du règlement exige que chaque responsable du traitement *prenne les mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé, la destruction, la perte, l'utilisation, la modification ou la divulgation de données à caractère personnel.*
20. Compte tenu de la nature sensible de ses activités en tant que banque, la CEB applique des politiques strictes en matière de sécurité des données. Celles-ci couvrent des domaines tels que le contrôle

d'accès, l'authentification, l'audit, la surveillance, les alertes, le stockage et la sauvegarde des données, les normes de transmission et l'intégrité de l'environnement. Le DPO étant également le responsable de la sécurité de l'information de la Banque, la sécurité des données est une priorité absolue. L'enquête que j'ai menée dans le cadre de la plainte décrite aux paragraphes 28 à 30 ci-dessous m'a permis d'observer les contrôles d'accès et autres mesures de sécurité appliqués aux données relatives aux ressources humaines, la principale catégorie de données à caractère personnel traitées par la Banque.

Violations de données

21. L'article 6.3, du règlement prévoit que toute violation de données doit être notifiée par le responsable du traitement concerné au Délégué à la protection des données, qui *notifie sans délai au Commissaire à la protection des données et à la (aux) personne(s) concernée(s) les violations de données susceptibles d'entraver gravement leurs droits et libertés fondamentaux*
22. Le 15 décembre 2023, le DPO m'a informé d'une violation de données. Il s'agissait d'un membre du personnel à qui l'on avait donné accès par inadvertance aux détails d'un formulaire de formation et de développement d'un collègue. Le membre du personnel concerné avait été informé de la violation, qui n'impliquait pas la divulgation de données sensibles. J'ai informé le DPO que j'étais satisfait des mesures prises, y compris les mesures d'atténuation mises en place pour éviter qu'une telle situation ne se reproduise.

Transferts de données à caractère personnel

23. L'article 12.1 du Règlement prévoit que *le transfert de données à caractère personnel en dehors de la Banque à un destinataire situé dans la juridiction d'un Etat ou d'une autre organisation internationale ne peut avoir lieu que si le/la Commissaire à la protection des données considère qu'un niveau de protection équivalent à celui du présent Règlement, qui est fondé sur les dispositions de la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel ("Convention 108+"), est assuré*. L'article 12.2 prévoit qu'*un tel niveau de protection peut être assuré par :*
    a) le droit de l'État ou de l'organisation internationale, y compris les traités ou accords internationaux applicables, en particulier le fait d'être partie à la Convention 108+ et d'en appliquer effectivement les dispositions ;
    b) des garanties standardisées ou ad hoc, approuvées par le/la Commissaire à la protection des données, établies par des instruments juridiquement contraignants et opposables, adoptés et mis en œuvre par les personnes impliquées dans le transfert et le traitement ultérieur des données, y compris des clauses contractuelles types et des dispositions à intégrer dans les arrangements administratifs entre les autorités ou les organismes publics.
24. Le 8 novembre 2022, j'ai délivré l'autorisation générale suivante, qui couvre la plupart des transferts de données à caractère personnel en dehors de la Banque :
    Conformément à l'article 12.1 du Règlement de la CEB sur la Protection des données, et compte tenu de l'article 12.2 (a) du Règlement, j'autorise le transfert de données à caractère personnel de la Banque à un destinataire lorsque ce destinataire est :

    a) dans la juridiction d'un État partie à la convention 108+ du Conseil de l'Europe, pour autant que cette convention soit entrée en vigueur ou
    b) dans la juridiction d'un État lié par le règlement général sur la protection des données (RGPD) de l'Union européenne ou
    c) relevant de la compétence d'un État, ou d'un secteur de cet État, pour lequel la Commission de l'Union européenne a décidé, conformément à l'article 45 du RGPD, que l'État ou le secteur assure un niveau de protection adéquat

    À condition que les données à caractère personnel aient par ailleurs été traitées conformément aux dispositions du règlement.
25. Le 3 novembre 2022, j'ai autorisé le transfert de données à caractère personnel de la Banque à l'OCDE dans le cadre de la décision de la Banque d'externaliser le traitement des salaires au SIRP, une agence de l'OCDE. En accordant cette autorisation, je me suis appuyé sur l'évaluation du DPO qui m'avait fourni un DPIA détaillé concernant les transferts en question.

26. Le 15 décembre 2023, j'ai autorisé le transfert de données à caractère personnel entre la Banque et le fournisseur d'un logiciel de publication basé aux États-Unis, afin de faciliter l'utilisation de ce logiciel dans la préparation des publications de la Banque. Ce transfert n'était pas couvert par l'autorisation générale décrite ci-dessus, car la société américaine n'avait pas pris l'engagement contraignant nécessaire pour se conformer aux exigences du *cadre de protection de la vie privée* UE-États-Unis. J'ai donné l'autorisation, en tenant compte des risques minimes encourus et à condition que le contrat entre la CEB et la société américaine comprenne des clauses juridiquement contraignantes et exécutoires garantissant un niveau de protection équivalent à celui prescrit par les règlements.

Plaintes

27. L'article 12.1 du Règlement prévoit que *toute personne concernée peut introduire une réclamation auprès du Commissaire à la protection des données si elle estime que les droits qui lui sont reconnus par le présent Règlement ont été violés*. Les autres parties de l'article 12 prévoient que le DPC examine la plainte et communique ses *conclusions motivées* au Gouverneur, qui prend une décision conformément à ces conclusions. Le plaignant peut faire appel de la décision du Gouverneur devant le Tribunal administratif.
28. Le 14 septembre 2022, la Banque a reçu une plainte d'un ancien membre du personnel, alléguant que la Banque avait violé les droits du membre du personnel en matière de protection des données. Le plaignant affirmait que, dans le cadre de l'emploi du membre au sein de la Banque, et plus particulièrement en ce qui concerne la cessation d'emploi du membre, des données à caractère personnel - y compris des catégories particulières de ces données - avaient été traitées d'une manière non conforme au Règlement. La plainte m'a été transmise le 8 octobre 2022.
29. Mon enquête sur la plainte a comporté un échange de correspondance avec le plaignant et avec la Banque, ainsi qu'un examen détaillé des dossiers pertinents de la Banque, sous forme électronique et physique. J'ai bénéficié d'un accès illimité à tous ces dossiers, y compris ceux détenus par les divisions RH, Juridique et Conformité. Mon examen m'a également permis de m'assurer des restrictions d'accès et des autres mesures de sécurité appliquées par la Banque à ces données à caractère personnel.
30. J'ai transmis mes conclusions au Gouverneur le 31 décembre 2022. Le résumé de mes conclusions était le suivant :
    Ayant examiné la plainte de X, ancien employé de la Banque ; agissant conformément à l'article 18.3 du Règlement de la CEB sur la Protection des données ; après avoir pris en considération les observations du plaignant et de la Banque ; après avoir examiné les dossiers pertinents de la Banque ; j'estime que le traitement par la Banque des données à caractère personnel du plaignant par les responsables du traitement concernés, pendant la période d'emploi du plaignant et jusqu'à ce jour, a été effectué en pleine conformité avec le Règlement sur la protection des données.
31. Mes conclusions ont été dûment communiquées au plaignant, qui n'a pas fait usage de son droit de recours devant le Tribunal administratif.
32. Le 21 novembre 2023, j'ai reçu du DPO une plainte d'un ancien membre du personnel selon laquelle son nom apparaissait en réponse à une recherche Google sur un aspect de ses interactions avec le Tribunal administratif, alors qu'il comprenait que le Tribunal lui avait donné l'anonymat. La question a été discutée de manière informelle avec le greffier du Tribunal pour que ce dernier y remédie.

Conclusion

33. Ce premier rapport en tant que Commissaire à la protection des données montre une organisation qui prend au sérieux ses responsabilités en tant que gardien des données personnelles. Le Règlement sur la protection des données de la CEB fixe le niveau élevé que l'on peut attendre d'un organisme qui fait partie de la famille du Conseil de l'Europe, avec son éminente réputation de promotion des normes les plus élevées de protection des données, considérées comme faisant partie du droit fondamental à la vie privée. La Banque a pris les mesures nécessaires pour s'assurer qu'elle sera pleinement conforme à ces règlements d'ici la fin de la période de transition, le 1er juillet 2024. À l'avenir, il faudra continuer à mettre l'accent sur la conformité de fond, car de nouveaux défis se posent dans le domaine de la protection des données. Le DPO, en collaboration avec ses collègues de la Banque, bénéficiera de mon soutien total dans cette tâche importante.