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

Rapport annuel du
Commissaire à la protection des données

1er janvier - 31 décembre 2024

RAPPORT ANNUEL DU COMMISSAIRE À LA PROTECTION DES DONNÉES 2024

(traduit de l'original en anglais)

Sommaire

Billy Hawkes

Janvier 2025

Résumé

Il s'agit de mon deuxième rapport en tant que Commissaire à la protection des données, qui couvre l'année 2024. Au cours de cette période, mon activité a été principalement axée sur la poursuite de la collaboration avec le délégué à la protection des données (DPO) veiller à ce que les exigences des Règlements, qui sont maintenant pleinement en vigueur, soient pleinement respectées. Au cours de l'année, je n'ai reçu aucune plainte de la part d'une personne concernée pour non-respect du règlement. Je n'ai pas non plus reçu de rapport faisant état d'une violation de données. Je pense que la Banque respecte en grande partie les normes élevées qu'elle s'est fixées dans les Règlements révisés et je suis convaincu qu'elle a mis en place des mesures pour résoudre le problème de la conservation des données qui subsiste. À l'avenir, la Banque est bien placée pour 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 deuxième rapport en tant que Commissaire à la protection des données, qui couvre l'année civile 2024. Il est établi conformément à l'article 17 du Règlement de la CEB sur la Protection des données, 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 12 mois, j'ai principalement travaillé avec le Délégué à la protection des données (DPO) pour consolider les progrès signalés dans mon premier rapport, afin de garantir le respect total des exigences des règlements, maintenant que ceux-ci sont pleinement en vigueur.

Visites à la Banque/contact avec le DPD

3. Je me suis rendu au siège de la Banque à Paris à trois reprises. Au cours ces visites, j'ai rencontré le Délégué à la protection des données, la Directrice du Bureau de la Conformité et la Direction des Affaires Juridiques pour discuter des progrès accomplis en vue de se conformer pleinement aux règlements. J'ai également rencontré les Chefs de l'Audit Interne et du Risque Opérationnel pour discuter de la pertinence de la protection des données à caractère personnel dans leurs domaines de compétence respectifs.
4. 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 noté que le DPO/RSSI et le Chef du Risque Opérationnel sont tous deux membres d'un Comité du Risque Opérationnel présidé par le Gouverneur. J'ai également noté que la protection des données était systématiquement prise en compte dans le cadre de la mission de l'Audit Interne.
5. Au cours de l'année, j'ai également eu des contacts avec le DPO sur des questions spécifiques pour lesquelles il m'a demandé conseil.

Règlement de la CEB sur la Protection des données

6. Le Règlement est entré en vigueur le 1er juillet 2022, après son approbation par le Conseil d'administration. Le Règlement a remplacé un système antérieur de protection des données qui était entré en vigueur en 2008. L'article 20 prévoit une période de transition de deux ans pour mettre les activités de traitement en conformité avec le Règlement. La période de transition a pris fin le 30 juin 2024, ce qui signifie que les obligations de conformité de la Banque au titre du Règlement sont désormais pleinement applicables.
7. Le Règlement prévoit un système complet de protection données à caractère personnel au sein de 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 indépendant externe.
8. 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, tout organe, toute institution ou toute autorité au sein de la Banque qui, seul(e) ou conjointement avec d'autres, a le pouvoir de décision en matière de traitement des données, que ce pouvoir découle d'un acte juridique ou de circonstances de fait*.

Rôle du commissaire

9. 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 missions et de ses pouvoirs conformément au présent Règlement et, ce faisant, ne sollicite ni n'accepte aucune instruction*. 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.
10. 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

11. 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 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 (tout comme la Directrice du Bureau de la Conformité, Katherine DELIKOURA).
12. 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

13. 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.

14. En prévision de l'entrée en vigueur du nouveau règlement, le DPO, avec l'aide d'un consultant, a 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 que le ROPA soit revu et mis à jour régulièrement.
15. 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.
16. L'un des aspects qui nécessite un travail plus approfondi est celui couvert par l'article 9, paragraphe 8, point f) : *les délais prévus pour l'effacement des différentes catégories de données.* Le transfert des données RH vers le système de planification des ressources de l'entreprise (ERP), prévu pour mi-2025, offre l'occasion d'intégrer ces délais dans les opérations RH de la Banque.
17. 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, a exigé que des modifications soient apportées à ces contrats au moment de leur renouvellement.

Transparence

18. 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 envisagé ;
    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 ;
    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.*
19. Une note détaillée a été diffusée à l'ensemble du personnel de la Banque le 27 novembre 2023. Elle contient les informations susmentionnées, y compris les rôles du DPO et du DPC. Cette note est également disponible sur l'intranet de la Banque.

Promotion de la sensibilisation et formation

20. L'article 14.2 (point j), du Règlement prévoit que l'une des tâches du DPO consiste *à promouvoir la sensibilisation au sein de la Banque aux principes de 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, 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)

21. L'article 9.4 du Règlement oblige les responsables du traitement à consulter le DPD *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 nature et du volume des données ou de la nature, de la portée et de la finalité du traitement, et le DP0 doit consulter le DPC dans les cas appropriés. Le DPO s'est fortement impliqué en conseillant les responsables du traitement dans la préparation de ces DPIA et m'a consulté le cas échéant.

Sécurité des données

22. 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.*
23. 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. Mon enquête sur la plainte décrite dans mon rapport 2023 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. Ces contrôles devraient être encore renforcés avec le transfert des données RH vers le système ERP.

Violations de données

24. L'article 6.5 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/à la Commissaire à la protection des données et à la/aux personne(s) concernée(s) les violations des données susceptibles d'entraver gravement leurs droits et libertés fondamentaux.* Aucune violation de ce type ne m'a été signalée en 2024.

Transferts de données à caractère personnel

25. L'article 12.1 du Règlement prévoit que *le transfert de données à caractère personnel en dehors de la Banque vers 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.*
26. 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 sur la protection des données de la CEB, 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.

27. Le 12 décembre 2024, j'ai autorisé le transfert de données à caractère personnel entre la Banque et le fournisseur d'un logiciel de gestion des performances basé aux États-Unis. Ce transfert n'était pas couvert par l'autorisation générale décrite ci-dessus car l'entreprise 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 accordé l'autorisation, en tenant compte de l'analyse d'impact sur la vie privée réalisée par la Banque et en étant convaincu que le contrat entre la CEB et la société américaine comprenait des clauses juridiquement contraignantes et exécutoires qui garantissaient un niveau de protection équivalent à celui prescrit par les règlements.

Engagement externe et visibilité

28. En septembre, j'ai rejoint le DPO et la Directrice de la Conformité à Washington D.C. pour l'atelier annuel sur la protection des données dans les organisations internationales. Organisée par la Banque mondiale, avec le soutien du Contrôleur européen de la protection des données, cette réunion s'est avérée une excellente occasion déchanger sur des sujets d'intérêt commun avec nos collègues d'autres organisations internationales. Mes collègues de la CEB ont ensuite participé au symposium annuel sur la protection des données des banques multilatérales de développement, qui s'est également tenu à Washington.
29. En octobre, j'ai assisté à la 46e réunion de l'Assemblée mondiale de la protection de la vie privée (GPA) à Jersey. Ce rassemblement annuel de commissaires à la protection des données et à la vie privée a abordé un large éventail de sujets lors de ses sessions publiques et restreintes, et a également offert des possibilités de réseautage informel.

Plaintes

30. L'article 18.1 du Règlement prévoit que *toute personne concernée peut déposer une réclamation auprès du/de la Commissaire à la protection des données si elle estime que ses droits au titre du présent Règlement ont été violés*. Les autres parties de l'article 18 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. Aucune plainte de ce type ne m'a été soumise en 2024.

Conclusion

31. Ce deuxième rapport en tant que Commissaire à la protection des données continue de montrer une organisation qui prend au sérieux ses responsabilités en tant que gardienne des données personnelles. Le Règlement sur la protection des données de la CEB fixe le niveau élevé que l'on est en droit d'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 en matière 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 est conforme à ces règlements, y compris les travaux en cours dans le domaine de la conservation des données. 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.