UNION POSTALE UNIVERSELLE

Bureau international
Weltpoststrasse 4
3015 BERNE
SUISSE

T +41 31 350 31 11
F +41 31 350 31 10
www.upu.int

Contact: Bonseung Ku
+41 31 350 35 24
bonseung.ku@upu.int

Aux opérateurs désignés des Pays-membres de l'Union

Berne, le 5 décembre 2023

Référence: 3911(DPRM.PPRE.PRA)1159
Objet: enquête sur les cadres réglementaires des Pays-membres de l'Union en matière de collecte et de protection des données

Madame, Monsieur,

Conformément à la Convention postale universelle, les Pays-membres sont tenus d'entreprendre un certain nombre d'activités liées aux échanges de données essentielles ou obligatoires. Les données échangées dans le cadre de ces activités sont souvent des données personnelles telles que les noms et les adresses physiques des expéditeurs et des destinataires.

Le cadre réglementaire actuel concernant la protection des données personnelles repose sur un certain nombre de dispositions énoncées dans la Convention et son Règlement ainsi que dans l'Arrangement concernant les services postaux de paiement et le cadre de l'Accord multilatéral de partage de données de l'UPU. Néanmoins, la plupart de ces dispositions reposent principalement sur la législation nationale de chaque Pays-membre. En outre, bien que l'accord précité prévoie des obligations spécifiques relatives à l'échange de données personnelles, le cadre n'est pas obligatoire, ce qui signifie qu'il reste des maillons de la chaîne logistique postale susceptibles d'être vulnérables aux violations de données et à d'autres formes d'abus.

Dans ce contexte, le Congrès d'Abidjan 2021 a décidé de conduire une enquête et une étude analytique sur les politiques et la réglementation en matière de collecte et de protection des données des Pays-membres de l'Union.[1] L'objectif est de comprendre les pratiques actuelles des opérateurs désignés en matière de protection des données personnelles. En s'appuyant sur cette compréhension, l'UPU vise à développer des services de conseil sur les réglementations destinés aux opérateurs désignés pour les aider à élaborer des cadres appropriés pour protéger le traitement et la transmission des données personnelles entre eux et les autres opérateurs désignés ou les autres acteurs du secteur postal élargi dans le contexte des opérations postales internationales. Les résultats de l'enquête seront également pris en considération dans le cadre de la révision des cadres réglementaires et politiques pour la collecte et la protection des données réalisée par le Conseil d'administration (CA).

[1] Proposition de travail 1.2.13 (Politique postale et régulation 1) du Plan d'activités d'Abidjan sur les obligations découlant des traités concernant le service universel, la régulation et la politique postale (v. résultats liés au pilier stratégique 132).

Dans le cadre de ce mandat, nous vous envoyons l'enquête ci-jointe, visant à recueillir des informations sur les cadres réglementaires des Pays-membres de l'Union concernant la collecte et la protection des données.
/ Veuillez répondre au questionnaire figurant en annexe 1 et le renvoyer au Bureau international le plus rapidement possible, **mais le 19 janvier 2024 au plus tard**. Les questionnaires de l'enquête sont également disponibles sur le site Web de l'UPU (https://www.upu.int/fr/espace-membres/politiques-et-regulation).

Veuillez agréer, Madame, Monsieur, l'assurance de ma haute considération.

Le Directeur des politiques, de la régulation
et des marchés,

Siva Somasundram

Enquête sur les politiques et la réglementation en matière de collecte et de protection des données utilisées dans le cadre du service postal international

Les opérateurs désignés des Pays-membres de l'Union sont priés de renvoyer ce questionnaire (sans lettre de couverture) le plus tôt possible, **mais le 19 janvier 2024 au plus tard,** à l'adresse suivante:

Bonseung Ku
Expert associé «Conseil en matière de politiques et de régulation»
Bureau international
Weltpoststrasse 4
3015 BERNE
SUISSE

Le questionnaire, dûment rempli, peut également être renvoyé par courrier électronique (bonseung.ku@upu.int).

Si vous rencontrez des difficultés en remplissant ce questionnaire, veuillez prendre contact avec Bonseung Ku au Bureau international (téléphone: (+41 31) 350 35 24; adresse électronique: bonseung.ku@upu.int).

❑ Ministère de tutelle (en charge du secteur postal) ❑ Régulateur (en charge du secteur postal) ❑ Opérateur désigné	
Nom de l'organisation	
Nom et prénom ❑ Mme ❑ M.	
Fonction/titre	
Adresse	
Pays	
Téléphone	Adresse électronique

Questionnaire

Partie I – Questions d'ordre général Oui Non

1. Dans le cadre de vos opérations postales nationales, à quelles réglementations en matière de protection des données/de la vie privée[1] êtes-vous soumis?

   - ❑ Règlement général sur la protection des données (réglementation de l'Union européenne)
   - ❑ Loi fédérale suisse sur la protection des données
   - ❑ Acte californien pour le respect de la vie privée des consommateurs
   - ❑ Loi générale de protection des données du Brésil
   - ❑ Aucune
   - ❑ Autre (veuillez préciser):

2. Y a-t-il des réglementations sur la protection des données spécifiques au secteur postal[2] dans votre pays? ❑ ❑

   Si oui, veuillez préciser:

3. Existe-t-il d'autres réglementations intersectorielles sur la protection des données, par exemple applicables aux douanes ou au transport, qui seraient également applicables au secteur postal dans votre pays? ❑ ❑

   Si oui, veuillez préciser:

4. À quelles fins recueillez-vous et échangez-vous des données personnelles[3] avec des tiers dans le cadre de l'exploitation des services postaux internationaux (veuillez sélectionner la ou les réponses correspondantes)?

   - ❑ Opérations (recueil, traitement, suivi/identification des envois, adressage, distribution, etc.)
   - ❑ Douanes et sécurité (telles que les données électroniques préalables (EAD) et les messages ITMATT)
   - ❑ Qualité de service (retours des clients, résultats en matière de distribution, etc.)
   - ❑ Finances et comptabilité (telles que les informations de facturation et les détails de paiement)
   - ❑ Autre (veuillez préciser):

[1] Le terme de «réglementations en matière de protection des données/de la vie privée» fait référence aux règles et normes gouvernant la manière dont les données personnelles sont recueillies, utilisées, stockées et transmises.
[2] Les réglementations spécifiques au secteur sont celles qui s'appliquent uniquement au secteur postal et peuvent prévoir des obligations différentes ou supplémentaires par rapport aux réglementations générales de la protection des données.
[3] Les données personnelles désignent toute information pouvant être utilisée pour identifier ou faire référence à une personne physique.

L'Accord multilatéral de partage de données de l'UPU, adopté par le Conseil d'exploitation postale en avril 2021, est un outil juridique créé pour faciliter l'échange des données nécessaires à l'exploitation des services postaux internationaux et permettre la mise en œuvre de ces échanges en accord avec les Actes de l'Union.

Cet accord intègre et étend les dispositions de fond des accords multilatéraux de partage de données existants établis à titre privé par les opérateurs désignés des Pays-membres de l'Union. Le but est de mieux refléter les obligations de partage de données pertinentes contenues dans les Actes de l'Union tout en établissant les conditions adéquates pour un outil à portée mondiale géré par l'UPU.

5. Êtes-vous signataire de l'Accord multilatéral de partage de données?

- ❑ Oui
- ❑ Non
- ❑ Autre (veuillez préciser):

Partie II – Responsabilité

6. Disposez-vous d'un responsable de la protection des données ou d'une personne similaire chargée de veiller à la conformité aux obligations en matière de protection des données et de la vie privée (veuillez sélectionner qu'une seule réponse)?

- ❑ Nous avons un responsable ou une équipe dédiée à la protection des données qui surveille et actualise régulièrement nos politiques et nos procédures
- ❑ Nous nous appuyons sur des consultants ou auditeurs externes qui examinent périodiquement nos politiques et procédures et nous conseillent à leur sujet
- ❑ Nous n'avons ni de responsable ni d'équipe dédiée à la protection des données qui surveille et actualise régulièrement nos politiques et nos procédures
- ❑ Autre (veuillez préciser):

7. Comment démontrez-vous votre responsabilité en matière de protection des données/de la vie privée à votre clientèle et à vos partenaires (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Nous publions notre politique et nos déclarations sur la protection des données sur notre site Web et d'autres canaux de communication
- ❑ Nous réalisons une évaluation et des audits réguliers des incidences de la protection des données[4] et rendons compte des résultats auprès de nos partenaires
- ❑ Nous n'avons pas de moyen spécifique de démontrer notre responsabilité en matière de confidentialité des données
- ❑ Autre (veuillez préciser):

[4] Une évaluation des incidences de la protection des données est un processus visant à identifier et à réduire les risques associés au traitement des données personnelles.

Partie III – Obligations d'information

8. Comment informez-vous les personnes visées par les données[5] des moyens utilisés pour traiter leurs données personnelles et des fins auxquelles elles sont traitées[6] (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Déclaration de confidentialité
- ❑ Conditions générales
- ❑ Adresse électronique
- ❑ Formules de consentement
- ❑ Les personnes visées par les données ne sont pas informées
- ❑ Autre (veuillez préciser):

9. Comment veillez-vous à ce que les données personnelles soient traitées uniquement aux fins pour lesquelles elles ont été recueillies (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Examen et actualisation réguliers des politiques de confidentialité et des formules de consentement pour qu'ils soient cohérents avec les objectifs spécifiques de la collecte de données
- ❑ Communication claire et transparente avec les personnes visées par les données concernant l'utilisation prévue de leurs données personnelles et obtention de leur consentement explicite pour toute fin supplémentaire
- ❑ Nous n'avons pas établi de méthode pour veiller à ce que les données personnelles soient traitées uniquement aux fins pour lesquelles elles ont été recueillies
- ❑ Autre (veuillez préciser):

Partie IV – Confidentialité et sécurité des échanges de données

10. Comment prévenez-vous la transmission non autorisée des informations confidentielles[7] (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Nous mettons régulièrement en place des programmes de formation et de sensibilisation sur les obligations en matière de protection des données/de la vie privée
- ❑ Nous disposons de politiques et de procédures écrites spécifiant les rôles et responsabilités des personnes traitant les données et les conséquences de leur non-respect
- ❑ Nous utilisons des mesures techniques et organisationnelles[8] pour protéger les informations confidentielles de tout accès, utilisation, modification ou diffusion non autorisé

[5] Les personnes visées par les données désignent toute personne physique pouvant être identifiée, directement ou indirectement, à l'aide de données telles qu'un nom, un identifiant ou des données de localisation, ou par des caractéristiques propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de la personne. En d'autres termes, une personne visée par les données est un utilisateur final dont les données personnelles peuvent être recueillies.

[6] Le traitement des données personnelles désigne toute opération ou tout ensemble d'opérations réalisées sur les données personnelles, telles que le recueil, le stockage, l'utilisation, la diffusion ou la suppression.

[7] La transmission non autorisée d'informations confidentielles signifie la diffusion ou l'utilisation d'informations réservées à certaines personnes ou entités.

[8] Les mesures techniques comprennent les mécanismes tels que le chiffrement ou les contrôles d'accès pour préserver les informations, et les mesures organisationnelles comprennent la mise en œuvre de procédures et de pratiques pour gérer et réduire les risques relatifs au traitement des données.

- ❑ Nous surveillons et évaluons les activités de traitement des données et signalons toute violation et tout incident aux autorités compétentes et aux parties intéressées
- ❑ Autre (veuillez préciser):

Concernant les questions 11 à 15, l'UPU reconnaît le fait que vous utilisez peut-être les technologies et services fournis par le Centre de technologies postales (CTP), en particulier IPS et le système de déclaration en douane (CDS), ainsi que, dans certains cas, l'hébergement de logiciels du CTP (tels que le nuage et .POST). Dans ce cas, une partie des réponses aux questions qui suivent peut venir des opérations du CTP. Nous vous demandons toutefois de bien vouloir répondre à ces questions et de compléter vos réponses avec les mesures que vous prenez localement.

11. Avez-vous un plan d'urgence[9] et un système de secours pour assurer la continuité du service et la reprise des activités en cas d'interruption non prévue ou de toute autre situation d'urgence (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Oui
    - ❑ Non
    - ❑ Autre (veuillez préciser):

12. Comment surveillez-vous et signalez-vous les violations de sécurité[10] relatives aux données personnelles échangées avec d'autres parties (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Nous avons une équipe ou une unité de sécurité dédiée qui surveille et signale toutes les violations de sécurité
    - ❑ Nous avons une politique ou une procédure prévoyant la réponse à une violation de sécurité qui guide nos activités de surveillance et de signalement
    - ❑ Nous nous appuyons sur les fonctionnalités de sécurité ou les alertes de nos systèmes ou réseaux pour détecter et signaler toute violation de sécurité
    - ❑ Nous ne surveillons pas et ne signalons pas les violations de sécurité
    - ❑ Autre (veuillez préciser):

13. Quelles parties notifiez-vous en cas de violation de sécurité (veuillez sélectionner la ou les réponses correspondantes)?
    - ❑ Bureau international de l'UPU
    - ❑ Autorités locales de protection des données
    - ❑ Personnes visées par les données affectées
    - ❑ Parties tierces affectées

[9] Un plan d'urgence est un ensemble de procédures et d'actions visant à prévenir toute menace ou interruption pouvant affecter les services postaux (telles que les catastrophes naturelles, les accidents ou les cyberattaques), à s'y préparer, à y réagir et à s'en rétablir.

[10] Une violation de sécurité est un événement compromettant la confidentialité, l'intégrité ou la disponibilité des données échangées avec d'autres parties tel qu'un accès, une diffusion ou une modification non autorisés, ou une perte ou une destruction.

- ❑ Nous ne notifions les violations de sécurité à personne
- ❑ Autre (veuillez préciser):

14. Dans quel délai notifiez-vous les parties concernées de la violation de sécurité (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Dans les vingt-quatre heures
    - ❑ Dans les soixante-douze heures
    - ❑ Dans la semaine
    - ❑ Un mois
    - ❑ Nous ne notifions pas les violations de sécurité
    - ❑ Autre (veuillez préciser):

15. À quelle fréquence réalisez-vous des audits ou des évaluations de sécurité[11] de l'infrastructure et de l'environnement d'exploitation utilisé pour l'échange de données avec des parties tierces (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Une fois par mois
    - ❑ Une fois par trimestre
    - ❑ Deux fois par an
    - ❑ Tous les ans
    - ❑ Jamais
    - ❑ Autre (veuillez préciser):

Partie V – Conservation des données

16. Comment déterminez-vous la durée de conservation des données[12] pour les données personnelles que vous traitez (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Nous respectons la durée de conservation pour notre juridiction locale
    - ❑ Nous respectons la durée de conservation correspondant à la juridiction la plus restrictive applicable
    - ❑ Nous conservons les données personnelles aussi longtemps que nécessaire
    - ❑ Nous conservons les données personnelles pour une période fixe de dix ans à partir de leur réception

[11] Les audits ou évaluations de sécurité sont des évaluations systématiques des politiques, procédures et contrôles qui protègent la confidentialité, l'intégrité et la disponibilité des données échangées avec d'autres parties.
[12] La période de conservation correspond à la durée pendant laquelle les données personnelles sont conservées aux fins de leur traitement, de leur stockage ou de leur archivage, avant qu'elles soient supprimées ou détruites de manière sécurisée.

- ❑ Autre (veuillez préciser):

17. Comment supprimez-vous les données personnelles[13] à la fin de la durée de conservation ou si elles ne sont plus nécessaires (veuillez sélectionner la ou les réponses correspondantes)?
    - ❑ Nous supprimons les données personnelles de tous les systèmes et services
    - ❑ Nous détruisons les données personnelles en les broyant, en les incinérant ou en les démagnétisant
    - ❑ Nous retournons les données personnelles à la partie expéditrice ou les transférons à un tiers autorisé par la partie expéditrice
    - ❑ Nous anonymisons ou agrégeons les données personnelles pour en supprimer toutes les informations personnelles ou sensibles
    - ❑ Nous conservons les données personnelles à des fins d'archivage, de recherche ou statistiques, avec les mesures de protection appropriées
    - ❑ Autre (veuillez préciser):

Partie VI – Droits d'accès

18. Quels types de droits d'accès offrez-vous pour les personnes visées par les données[14] (veuillez sélectionner la ou les réponses correspondantes)?
    - ❑ Droit d'accès
    - ❑ Droit de rectification
    - ❑ Droit de suppression
    - ❑ Droit à la portabilité des données
    - ❑ Droit à objecter
    - ❑ Droit de restreindre le traitement
    - ❑ Pas de droits spécifiques accordés
    - ❑ Autre (veuillez préciser):

[13] La suppression des données personnelles signifie la suppression, la destruction ou l'anonymisation des données personnelles de manière sécurisée et irréversible afin qu'elles ne puissent plus être accédées, stockées ou diffusées par des parties non autorisées.

[14] Les droits d'accès par les personnes visées par les données sont les droits dont les personnes physiques disposent d'accéder, de corriger, de supprimer ou de restreindre le traitement de leurs données personnelles détenues par une organisation.

19. Dans quel délai répondez-vous[15] aux demandes ou aux requêtes de parties tierces ou des personnes visées par les données (veuillez ne sélectionner qu'une seule réponse)?

- ❑ Un jour calendaire
- ❑ Un à trois jours calendaires
- ❑ Quatre à sept jours calendaires
- ❑ Deux ou trois semaines
- ❑ Un mois
- ❑ Pas de délai spécifique
- ❑ Autre (veuillez préciser):

20. Quel est votre processus[16] pour la réponse aux demandes d'information de tiers ou des personnes visées par les données (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Nous avons une politique et une procédure formelles d'évaluation et de réponse aux demandes d'information émises par des tiers et nous documentons et suivons toutes les demandes et réponses
- ❑ Nous avons des grandes lignes directrices concernant la réponse aux demandes d'information émises par des tiers, mais nous n'avons ni politique ni procédure formelle et nous de documentons pas et ne suivons pas les demandes et les réponses
- ❑ Nous n'avons pas de processus spécifique pour répondre aux demandes d'information émises par des tiers et nous les traitons au cas par cas selon la nature et l'origine de la demande
- ❑ Nous ne répondons pas aux demandes d'information émises par des tiers, sauf en cas d'obligation juridique
- ❑ Autre (veuillez préciser):

Partie VII – Registre des activités de traitement des données

21. Comment tenez-vous un registre des activités de traitement des données[17]? Quels sont le format et la structure généraux de vos registres des activités de traitement des données (veuillez ne sélectionner qu'une seule réponse)?

- ❑ Nous utilisons un logiciel ou un outil dédié
- ❑ Nous utilisons une feuille de calcul ou un document
- ❑ Nous utilisons un journal physique ou électronique
- ❑ Nous ne tenons pas de registre des activités de traitement des données

[15] Une réponse est une communication qui reconnaît, répond à ou assure le suivi d'une demande ou d'une requête émise par un tiers, par exemple par courrier ou par courrier électronique.
[16] Les processus sont des demandes d'information de tiers pouvant nécessiter la réception, la vérification, la hiérarchisation, l'attribution, la récupération, la compilation, l'examen, l'approbation et l'envoi des informations.
[17] Les registres des activités de traitement des données sont des documents ou des registres qui décrivent les données personnelles que vous recueillez, utilisez, stockez et communiquez en tant qu'opérateur désigné.

- ❑ Autre (veuillez préciser):

22. Pour quelles informations relatives aux activités de traitement des données tenez-vous un registre (veuillez sélectionner la ou les réponses correspondantes)?
    - ❑ Nom et coordonnées de chaque partie traitant les données
    - ❑ Catégories et sources des données traitées
    - ❑ Description des mesures de sécurité techniques et organisationnelles
    - ❑ Autre (veuillez préciser):

23. À quelle fréquence révisez-vous et actualisez-vous votre registre des activités de traitement des données (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Au moins une fois par an.
    - ❑ Tous les six mois
    - ❑ Tous les trois mois
    - ❑ Plus souvent que tous les trois mois
    - ❑ Jamais ou rarement
    - ❑ Autre (veuillez préciser):

Partie VIII – Formation et sensibilisation

24. Votre organisation forme-t-elle son personnel à la protection des données[18] (veuillez ne sélectionner qu'une seule réponse)?
    - ❑ Oui, nous avons des programmes de formation réguliers et complets sur la protection des données pour tous les membres du personnel
    - ❑ Oui, mais les formations sont minimes et ne sont pas souvent mises à jour
    - ❑ Non, notre organisation ne propose actuellement pas de formation sur la protection des données à son personnel
    - ❑ Autre (veuillez préciser):

[18] Les formations peuvent comprendre toutes les méthodes visant à former les membres du personnel sur les principes, processus et responsabilités applicables au sujet de la protection des données/de la vie privée, y compris des sessions de formation en direct, des formations en ligne, des ressources et des supports, etc.

Partie IX – Expérience pratique

25. Avez-vous déjà rencontré des difficultés ou des défis[19] dans la collecte, le traitement, la transmission ou la réception de données (veuillez ne sélectionner qu'une seule réponse)?

- ❑ Oui, fréquemment
- ❑ Oui, occasionnellement
- ❑ Non, jamais
- ❑ Je ne sais pas
- ❑ Autre (veuillez préciser):

26. Si vous avez répondu oui à la question précédente, quelles ont été les principales causes ou sources des difficultés ou des défis rencontrés (veuillez sélectionner la ou les réponses correspondantes)?

- ❑ Normes ou systèmes techniques incompatibles ou obsolètes
- ❑ Manque de clarté ou de cohérence dans les exigences ou les formats applicables aux données
- ❑ Barrières ou restrictions juridiques ou réglementaires
- ❑ Erreurs ou retards humains ou opérationnels
- ❑ Autre (veuillez préciser):

[19] Les difficultés et les défis peuvent porter sur des problèmes techniques, la qualité des données, les problèmes, la sécurité des données, les violations de la confidentialité, les régulateurs ou les barrières juridiques.