Position sur le deuxième rapport de la Commission européenne sur l'application du règlement général sur la protection des données

PostEurop

Publié par **POSTEUROP**
Bruxelles, 28 novembre 2024
Registre de Transparence : 092682012915-24

PostEurop

À propos de POSTEUROP

POSTEUROP est l'association qui représente les opérateurs postaux européens depuis 1993 et est officiellement reconnue comme une Union restreinte de l'Union postale universelle (UPU).

Elle s'engage à soutenir et à développer un marché européen des communications postales durable et compétitif, accessible à tous les citoyens et garantissant un service universel moderne et abordable.

Ses membres emploient **1,6 million de personnes** et distribuent chaque année des milliards d'envois à plus de **295 millions de foyers** et **48 millions d'entreprises en Europe.**

Association des opérateurs postaux publics européens AISBL

Boulevard Brand Whitlock 114
1200 Bruxelles
Belgique

T : + 32 2 761 9650
E : info@posteurop.org

CONTEXTE

PostEurop soutient l'examen en cours de l'application du RGPD ainsi que des défis qui en découlent.

PostEurop reconnaît les objectifs et les avantages du cadre du RGPD visant à encourager le développement d'un cadre cohérent et fiable de protection des données, dans l'intérêt des citoyens et de la société en général.

Cependant, il est essentiel que ce cadre soit clair, prévisible et opérationnel. Le RGPD doit apporter « une sécurité juridique et pratique aux opérateurs économiques et aux autorités publiques ».

La conformité au RGPD dans le cadre réglementaire européen plus large et en évolution rapide, tant d'un point de vue technologique qu'économique, risque de devenir extrêmement difficile si les prestataires du service postal universel doivent continuer à fournir des services postaux durables et prospères, et garantir la contribution économique de ces services postaux et de ces prestataires de services.

Notre contribution se concentre sur les parties du rapport qui sont les plus pertinentes pour les aspects de la protection des données affectant notre activité postale et d'autres services connexes aux utilisateurs postaux.

PostEurop souhaite notamment que l'application du RGPD prenne en compte les spécificités du secteur des services postaux, qui découlent des objectifs sociaux, culturels et économiques inhérents à la fourniture de services répondant aux besoins des utilisateurs postaux. Il plaide également pour un niveau élevé de cohérence par rapport au cadre législatif européen plus large en matière de numérique et de données, afin de garantir que l'innovation et l'évolution des services postaux ne soient pas compromises.

PostEurop soutient les conclusions et recommandations suivantes dans le rapport[1]:

L'EDPB et les DPA sont invités à :

- Engager un dialogue constructif avec les responsables du traitement et les sous-traitants sur la conformité au RGPD.
- Étudier les moyens/outils permettant d'aider davantage les exportateurs de données dans leurs efforts de mise en conformité avec les exigences de la directive Schrems II.
- Établir une coopération régulière avec d'autres régulateurs sectoriels sur des questions ayant un impact sur la protection des données, en particulier ceux établis dans le cadre de la nouvelle législation numérique de l'UE, et participer activement aux structures au niveau de l'UE conçues pour faciliter la coopération interréglementaire.
- Faire un usage plus complet des outils de coopération prévus par le RGPD, de sorte que la résolution des litiges ne soit utilisée qu'en dernier recours.
- Mettre en œuvre des modalités de travail plus efficaces et plus ciblées pour les lignes directrices, les avis et les décisions, et donner la priorité aux questions clés afin de réduire la charge qui pèse sur les autorités chargées de la protection des données et de répondre plus rapidement aux évolutions du marché.

La Commission s'engage à :

- Créer des synergies et une cohérence entre le RGPD et l'ensemble de la législation relative au traitement des données à caractère personnel sur la base de l'expérience acquise et, si nécessaire, prendre des mesures appropriées pour assurer la sécurité juridique
- Réfléchir à la manière de mieux répondre à la nécessité d'une coopération interréglementaire structurée et efficace pour garantir l'application effective, cohérente et homogène des règles numériques de l'UE, tout en respectant la compétence des autorités chargées de la protection des données pour toutes les questions relatives au traitement des données à caractère personnel.
- Utiliser tous les moyens disponibles pour fournir des éclaircissements rapides sur les questions importantes pour les parties prenantes, notamment en demandant l'avis du conseil d'administration.
- Coopérer avec les partenaires internationaux pour faciliter les flux de données - y compris s'ils sont effectués sur la base de clauses contractuelles types.

[1] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL - Deuxième rapport sur l'application du règlement général sur la protection des données COM/2024/357 final (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52024DC0357)

- Soutenir les processus de réforme en cours dans les pays tiers concernant les règles de protection des données nouvelles ou modernisées en partageant l'expérience et les meilleures pratiques.
- Collaborer avec des organisations internationales et régionales telles que l'OCDE et le G7 pour promouvoir des flux de données fiables fondés sur des normes élevées de protection des données, notamment dans le cadre de l'initiative « Libre Flux de données en toute confiance ».

COMMENTAIRES GÉNÉRAUX DE POSTEUROP SUR LE RGPD

Équilibre entre les droits fondamentaux et les principes clés

Le RGPD précise que les droits fondamentaux à la vie privée et à la protection des données doivent être mis en balance avec d'autres droits fondamentaux. Il s'agit notamment du droit d'exercer des activités commerciales légitimes et du droit des citoyens de l'UE de bénéficier de services d'intérêt économique général.

Ces principes généraux doivent être reconnus dans les approches de mise en œuvre. La confiance dans le consentement de la personne concernée ne doit pas devenir la position par défaut. Cela reviendrait à ignorer l'équilibre des droits clairement envisagé par le RGPD, ainsi que la responsabilité du responsable du traitement et les autres bases légales explicitement prévues.

PostEurop reconnaît l'importance de la Charte des droits fondamentaux et de la Convention européenne des droits de l'homme dans ce domaine. Ces instruments protègent également un large éventail de droits et d'intérêts, qui doivent tous être équilibrés de manière efficace.

Complexité et coût

La complexité et le coût représentent des défis importants pour la mise en conformité des entreprises avec le cadre du RGPD, même pour les grandes entités.

Les entreprises éprouvent des difficultés à gérer l'interaction entre le RGPD et d'autres instruments législatifs ou réglementaires affectant l'utilisation des données personnelles, y compris la réglementation des droits des consommateurs, des services numériques, des technologies spécifiques, de la cybersécurité et de l'utilisation des données non personnelles.

L'importance des services postaux pour les consommateurs et les entreprises demeure, alors que des innovations sont simultanément nécessaires pour répondre aux besoins changeants des utilisateurs. L'incertitude demeure en ce qui concerne les définitions clés, les cadres qui se chevauchent et les approches potentielles en matière de mise en œuvre. Il en résulte un paysage réglementaire complexe. Il est également contraire au principe juridique et réglementaire de base selon lequel les entreprises devraient être en mesure de planifier leurs activités en ayant une connaissance claire des conséquences juridiques.

Les lignes directrices qui sont théoriques ou qui se contentent de rappeler la loi ne suffisent pas ; il faut des conseils sur les solutions pratiques qui sont acceptables, et ce en temps opportun.

Approche fondée sur les risques

Le principe de responsabilité et l'approche fondée sur les risques reflètent une application souple des principes de protection des données tout en reconnaissant la responsabilité des responsables du traitement. Les considérants 74 et 76 du RGPD indiquent clairement que les responsables du traitement doivent évaluer la probabilité et la gravité du risque pour les droits et libertés des personnes concernées.

Le défi que pose la mise en œuvre d'une approche fondée sur les risques dans le cadre de la conformité au RGPD est l'obligation non seulement de tenir compte des risques pour le responsable du traitement/l'opérateur économique, mais aussi de prendre dûment en considération les droits et les libertés des personnes concernées.

Il est extrêmement difficile de mettre cela en pratique.

Si les orientations indiquent clairement qu'une DPIA doit être une véritable évaluation des risques, elles autorisent également les responsables du traitement à prendre des mesures pour y faire face. Toutefois, il existe peu d'orientations sur la manière d'évaluer réellement la nécessité et la proportionnalité, ni sur les outils pratiques nécessaires pour gérer tout risque identifié pour les droits et libertés des personnes concernées résultant du traitement des données à caractère personnel.

Dans le même temps, il est nécessaire de fournir davantage d'orientations et de clarté sur des aspects spécifiques des droits des personnes concernées, tels que la protection des droits des mineurs. Dans son rapport, la Commission indique que les enfants ont besoin d'une protection spécifique lorsque leurs données à caractère personnel sont traitées et que l'accent est mis de plus en plus sur la nécessité de disposer d'outils de vérification de l'âge efficaces et respectueux de la vie privée. Il est important que les travaux lancés par la Commission européenne début 2024 sur le sujet progressent rapidement.

Un besoin évident de cohérence

Il existe un réel besoin de cohérence, notamment en ce qui concerne les décisions des autorités de contrôle, qui conduisent souvent à une interprétation restrictive du RGPD, mais aussi en ce qui concerne l'articulation entre le RGPD et les nouvelles obligations découlant de la stratégie numérique européenne.

Le RGPD marque la volonté d'harmonisation au niveau européen. Il vise à renforcer les droits des citoyens européens, mais aussi à responsabiliser les entreprises et les organisations qui traitent des données personnelles. Cependant, il renvoie à des cadres nationaux, ce qui risque inévitablement de conduire à des différences d'application entre les autorités de protection des données des États membres. PostEurop note que ces variations ont été reconnues dans le rapport et qu'il a conduit à un plus grand niveau d'incohérence et de fragmentation que les mesures législatives nationales spécifiques.

Une interprétation souvent restrictive du RGPD

La possibilité de mener des consultations constructives avec les autorités chargées de la protection des données favoriserait le respect du règlement, de même que des consultations publiques plus significatives de la part de l'EDPB.

Les lignes directrices restreignent parfois de manière excessive la marge de manœuvre laissée par le RGPD, notamment pour les questions liées au régime de protection de la vie privée en ligne. En conséquence, de nombreuses entreprises appliquent un principe de précaution et hésitent à se lancer dans des projets qui semblent trop complexes ou trop coûteux à mettre en œuvre compte tenu des nombreuses contraintes liées au RGPD.

Le rapport a clairement identifié les préoccupations à cet égard et PostEurop soutient les points suivants :

- Les autorités de contrôle devraient engager un dialogue constructif avec les responsables du traitement des données et les sous-traitants sur le respect du RGPD ; et les lignes directrices au niveau des Etats membres devraient refléter les orientations ou les avis émis au niveau de l'UE, ainsi que la jurisprudence de la Cour de justice ;
- Les consultations sur les lignes directrices et les avis visent à comprendre les réalités opérationnelles et économiques, ainsi que les implications pratiques pour les entreprises concernées ;
- Des lignes directrices plus courtes, pragmatiques et accessibles fournissant des orientations claires et sans ambiguïté sur l'application du RGPD soient disponibles ; et qu'elles soient également mises à jour pour tenir compte de l'expérience, des développements technologiques ou des évolutions juridiques.

Des orientations actualisées font actuellement défaut sur certaines questions essentielles, comme le concept de « données à caractère personnel », qui évolue à la lumière de la jurisprudence récente de la CJUE et risque de manquer de clarté.

Il existe également un risque émergent de conflit entre les concepts de « données ouvertes » dans la politique des données de l'UE et les objectifs en matière de données à caractère personnel. Compte tenu de la réglementation accrue des données non personnelles, une définition plus claire et plus prévisible de ce qui constitue les données personnelles est essentielle.

En outre, ce qui constitue un « transfert » peut même ne pas être sûr[2].

Des conseils sur les solutions pratiques, techniques et réalisables pour les opérateurs économiques sont essentiels pour assurer la conformité.

[2] Une décision récente du CEPD concernant l'utilisation d'un logiciel de vidéoconférence par la CJUE (basée sur le règlement (UE) 2018/172519) a estimé que, puisque l'importateur de données était contractuellement exclu de l'accès aux données à caractère personnel traitées par l'exportateur de données et que ces données étaient cryptées, il n'y avait pas de transfert de données au sens de la législation de l'UE en matière de protection des données. Décision du CEPD relative à la demande de la Cour de justice de l'UE d'autoriser les clauses contractuelles entre la Cour de justice de l'UE et Cisco Systems Inc. pour les transferts de données à caractère personnel dans le cadre de l'utilisation par la Cour de Cisco Webex et des services connexes, 13 juillet 2023, dossier 2023-0367.

Nouveaux défis juridiques pour la sécurité des données

Pierre angulaire de la réglementation européenne en matière de protection des données à caractère personnel, le RGPD est désormais intégré aux nouvelles obligations découlant de la stratégie numérique de l'Europe, telles que la loi sur les marchés numériques, la loi sur la gouvernance des données et la loi sur l'intelligence artificielle.

À l'avenir, il sera toutefois nécessaire d'assurer la cohérence de la réglementation de l'espace numérique européen. PostEurop note que cela a été clairement reconnu dans le rapport.

L'imbrication des enjeux et des défis peut parfois conduire à des contradictions ou à des blocages qui nuisent nécessairement aux objectifs recherchés. Les nouvelles utilisations des données et l'accélération de la numérisation au sein des organisations et des entreprises favorisent le traitement de quantités croissantes de données, augmentant ainsi le risque pour la vie privée et la sécurité des données.

Difficultés récurrentes rencontrées lors du transfert de données en dehors de l'Espace économique européen (EEE)

Le transfert de données à caractère personnel en dehors de l'Espace économique européen (EEE) est devenu un défi majeur pour la plupart des organisations. L'annulation des décisions d'adéquation antérieures, ainsi que les contestations en cours, ont entraîné une grande incertitude juridique quant aux solutions et mécanismes qui seront acceptés par les autorités nationales de protection des données, l'EDPB et les tribunaux.

Le concept clé selon lequel l'approche fondée sur le risque s'applique à l'ensemble des obligations des responsables du traitement et des sous-traitants, y compris le chapitre V du RGPD (transferts internationaux), devrait être clairement reconnu.

PostEurop note que la nécessité de prendre en compte la nature spécifique du transfert, ainsi que les défis qui se posent encore dans les transferts internationaux, ont été clairement reconnus dans le rapport. PostEurop convient qu'il est nécessaire de reconnaître les besoins et caractéristiques uniques dans l'application du chapitre V du RGPD sur les transferts internationaux de données.

Les incohérences dans l'approche devraient également être résolues. Par exemple, l'application d'une approche fondée sur le risque en tenant compte des droits et libertés des personnes concernées est évidente dans les lignes directrices publiées sur les DPIA (bien qu'elles manquent d'orientations spécifiques) et pourtant l'approche reste peu claire et incertaine dans les lignes directrices sur les transferts internationaux de données.

L'obligation d'envisager des mesures de protection supplémentaires (en s'appuyant sur les CSC) est extrêmement difficile à mettre en pratique. La charge que représente pour les opérateurs économiques l'évaluation de la législation nationale dans les pays n'appartenant pas à l'EEE est disproportionnée. L'absence d'orientations claires et réalistes dans ce domaine ne tient pas compte des réalités et des besoins des prestataires de services interconnectés au niveau mondial.

Il est difficile de choisir entre les différentes mesures proposées par l'EDPB. En effet, si l'accès aux données à caractère personnel par les autorités publiques est autorisé dans le pays importateur, des mesures techniques (en particulier le cryptage) doivent être envisagées. Toutefois, des orientations sont nécessaires pour soutenir la mise en œuvre des préoccupations en matière de protection de la vie privée et refléter les réalités économiques pratiques d'une situation donnée. Le rapport reconnaît que les caractéristiques spécifiques de chaque transfert peuvent différer, mais il n'est pas clair comment placer le curseur entre les différentes catégories de données transférées.

Une approche plus pragmatique et innovante pourrait être nécessaire de manière plus générale en ce qui concerne les transferts internationaux de données.

PostEurop se félicite du soutien apporté aux efforts déployés au niveau intergouvernemental. Des questions telles que la réglementation de l'accès gouvernemental ne sont pas faciles à traiter au niveau des opérateurs économiques.

PostEurop note également que le besoin d'une orientation pratique sur les évaluations de l'impact des transferts, ainsi qu'une approche plus harmonisée, ont été pris en compte dans le rapport. [3]

Enfin, des solutions sont nécessaires pour concilier la défense des valeurs européennes, telles que la protection des citoyens et de leurs données, avec le développement numérique des entreprises européennes :

[3] Rapport, pages 22-23.

- Les décideurs politiques et les autorités de protection des données de l'UE devraient fournir des orientations supplémentaires sur la question des transferts illégaux. Des analyses différentes ne favorisent pas les transferts de données juridiquement sûrs.
- La mise en place de mécanismes de contrôle par des tiers, y compris des normes internationalement reconnues, pourrait permettre de vérifier que l'importateur respecte les conditions contractuelles du transfert et les mesures de sécurité.
- Les autorités de contrôle devraient également être plus claires et préciser leur position sur la question des transferts.

Améliorations nécessaires pour permettre l'identification des acteurs

Les mesures institutionnelles doivent être recentrées afin de garantir que les opérateurs économiques concernés puissent agir dans le cadre de paramètres clairs, pratiques et prévisibles et que les principales préoccupations pratiques soient prises en compte.

La classification juridique des différents acteurs peut encore donner lieu à une grande incertitude juridique.

La jurisprudence sur les contrôleurs conjoints évolue, mais la position sur la responsabilité de chaque partie reste vague en termes pratiques.

Il conviendrait de définir plus clairement la manière dont les responsabilités des différents responsables du traitement devraient être différenciées et délimitées en cas de contrôle conjoint. PostEurop note que le rapport a reconnu la nécessité de clarifier les différents rôles.

Enfin, la position des acteurs économiques qui fournissent les solutions techniques devrait être examinée de plus près.

Ces prestataires ne devraient pas inévitablement se retrouver dans la position d'un sous-traitant au sens du RGPD, même lorsqu'il a clairement déterminé toutes les finalités et tous les moyens du traitement lié à son service. Les fournisseurs de ces services ne souhaitent pas être qualifiés de responsables du traitement. Il conviendrait d'apporter des réponses concrètes à cette question.

PostEurop apprécie l'opportunité de soumettre des commentaires sur le rapport de la Commission.

Pour en savoir plus, veuillez contacter :

Mlle Christelle Defaye-Geneste

Présidente du Comité Affaires de l'Union européenne
La Poste Groupe

E : christelle.geneste@laposte.fr
T : +33 155 440 181

Mlle Sarah Gallagher

Présidente du Groupe de Travail Protection des données
An Post

E : sarah.gallagher@anpost.ie
T : +353 1 705 8432

Crédits photos : istock

Contact POSTEUROP :

Association des Opérateurs postaux publics européens
AISBL

Boulevard Brand Whitlock 114
1200 Bruxelles
Belgique

E : info@posteurop.org

T : + 32 2 761 9650