LA POSTE
GROUPE

Position du groupe La Poste
EDPB DPIA Template

EN RÉSUMÉ

Le groupe La Poste soutient l'initiative de l'EDPB visant à harmoniser les analyses d'impact relatives à la protection des données (AIPD) à travers un modèle (*template)* commun, susceptible d'améliorer la cohérence, la lisibilité et la comparabilité des pratiques au sein de l'Union européenne.

Toutefois, dans des environnements multiservices et multi-entités caractérisés par des traitements complexes, industrialisés et impliquant de nombreux acteurs, le groupe souligne la nécessité de garantir un modèle à la fois opérable, proportionné et soutenable dans la durée.

Dans cette perspective, plusieurs points de vigilance sont identifiés :

- La capacité du *template* à refléter de manière globale et cohérente les chaînes de responsabilité et les flux de données dans des écosystèmes multi-acteurs ;
- L'intégration opérationnelle de l'AIPD dans les processus existants (notamment la gestion des changements IT, la gestion des versions et la contribution des sous-traitants) ;
- La nécessité d'un niveau de granularité adapté, évitant une documentation trop technique ou redondante au regard de l'objectif de maîtrise des risques ;
- L'encadrement des usages secondaires des données et des analyses de compatibilité ;

- La clarification des bases légales et de leur articulation avec l'analyse de nécessité et de proportionnalité ;
- Le renforcement du caractère opérationnel des exigences en matière de « *privacy by design* » et d'évaluation de la nécessité ;
- L'harmonisation des méthodes d'évaluation des risques afin de limiter les divergences d'interprétation ;
- L'adaptation de certaines exigences (consultation des parties prenantes, consultation préalable des autorités) aux traitements complexes ou infrastructurels.

Sur cette base, le groupe La Poste formule des recommandations visant à renforcer le caractère opérationnel du *template*, à mieux articuler celui-ci avec les dispositifs existants (notamment le registre des traitements) et à garantir une mise en œuvre proportionnée et adaptée aux organisations complexes.

Le groupe La Poste accueille favorablement l'initiative de l'EDPB visant à harmoniser la documentation des analyses d'impact relatives à la protection des données (AIPD) au niveau européen au moyen d'un modèle *(template)* commun, accompagné d'un document explicatif. Une telle harmonisation est susceptible d'améliorer la cohérence des pratiques et de faciliter, pour les organisations opérant dans plusieurs États membres, la comparabilité et la lisibilité des analyses AIPD. Ce *template* vise également à harmoniser les attentes des autorités de contrôle européennes, à standardiser les modalités de démonstration de l'*accountability* et à faciliter la conduite d'AIPD dans un contexte transfrontière.

Toutefois, au regard de la diversité des activités d'un groupe multiservices (services postaux/logistiques, services financiers, services numériques de confiance, SI mutualisés), il apparaît important que le *template* demeure opérable, proportionné et adaptable à des traitements complexes, multi-acteurs et fortement industrialisés, sans générer de redondances excessives et de charge documentaire déconnectée de l'objectif de maîtrise effective des risques et en garantissant la soutenabilité du dispositif dans le temps pour des organisations multi-entités.

À ce titre, les principaux points de vigilance identifiés dans le *template* sont détaillés ci-après.

1. Cartographie des rôles : responsables de traitement conjoints/chaînes de sous-traitance (rubriques 0.1-0.2)

Dans les écosystèmes numériques (identité numérique, signature électronique, archivage électronique, plateformes), les schémas de responsabilité impliquent souvent des situations de responsabilité conjointe, de co-traitance ou de sous-traitance en chaîne (intégrateurs, hébergeurs/cloud, services managés, éditeurs).

Le *template* prévoit une description structurée des responsables de traitement et des sous-traitants, incluant leurs obligations et missions. Toutefois, cette approche, principalement organisée par acteur, peut conduire à une représentation fragmentée du traitement, appréhendé comme une juxtaposition de relations bilatérales.

À cet égard, il pourrait être utile de renforcer la description du traitement dans sa

dimension globale, en articulant de manière plus explicite les flux de données, le rôle effectif de chaque acteur et les interactions entre les différents sous-traitants tout au long de la chaîne de traitement.

Dans cette perspective, une attention particulière pourrait également être portée à certaines exigences complémentaires, notamment :

- La réalisation d'une cartographie complète des sous-traitants et sous-traitants ultérieurs, reflétant l'ensemble de la chaîne de traitement, dans la mesure où le responsable de traitement demeure responsable de l'ensemble des opérations qui y sont effectuées ;
- L'identification du lieu d'implantation de ces acteurs, afin de déterminer précisément où les données sont traitées et, le cas échéant, d'évaluer les transferts de données hors de l'Union européenne.

Dans un groupe multiservices tel que La Poste, les traitements de données personnelles reposent largement sur des systèmes d'information mutualisés entre entités métiers, ainsi que sur des chaînes de prestataires impliquant des acteurs multiples (*cloud*, infogérance, éditeurs, intégrateurs). Dans ce contexte, la démonstration de la conformité au Règlement général sur la protection des données (RGPD) ne dépend pas uniquement de l'existence de mesures techniques ou organisationnelles, mais de la capacité à documenter de manière claire, cohérente et opérationnelle la répartition effective des responsabilités entre responsables de traitement, responsables de traitement conjoints et sous-traitants. La clarté de la chaîne de responsabilité constitue ainsi un élément déterminant de l'*accountability*, en particulier pour des traitements complexes et industrialisés et doit pouvoir être correctement appréhendée et documentée dans le cadre du *template* de l'AIPD proposé.

Le groupe La Poste recommande :

- ***D'ajouter un encart explicite permettant de décrire (i) la mise en œuvre opérationnelle des obligations du RGPD entre entités (information, droits, sécurité, incidents, transferts, conservation), (ii) les flux inter-entités et (iii) les responsabilités opérationnelles sur les mesures de mitigation.***
- ***De prévoir, à titre facultatif, un champ « structure de gouvernance » du traitement afin de permettre de décrire, lorsque l'AIPD le justifie, la description de l'organisation opérationnelle associée (instances de gouvernance, répartition des rôles – par exemple sous forme de RACI – et modalités de pilotage). Ce champ serait particulièrement utile dans les environnements multi entités ou présentant une complexité organisationnelle spécifique.***

2. Ajout relatif à la section 0.5 « fiche technique de l'AIPD »

Le *template* de l'EDPB souligne la nécessité de justifier précisément le recours à une AIPD, et d'assurer la traçabilité des évolutions du traitement. Dans cette logique, l'AIPD est conçue comme un document vivant, appelé à évoluer en fonction des transformations du traitement, qu'elles soient techniques, organisationnelles ou contractuelles.

Toutefois, le *template* ne précise pas suffisamment les modalités d'intégration de cette exigence dans les processus opérationnels existants des organisations, notamment en lien avec la gestion des changements IT et l'évolution des chaînes de sous-traitance.

Le groupe La Poste recommande :

- ***De compléter la section 0.5 « fiche technique de l'AIPD » afin de préciser :***
  - ***L'articulation avec les processus internes de gestion des changements IT ;***
  - ***Les événements déclencheurs d'une mise à jour (tels que le recours à de nouveaux sous-traitants, l'évolution des finalités ou des modifications technologiques) ;***
  - ***Les modalités permettant d'assurer le maintien et la mise à jour de l'AIPD dans la durée, au sein d'environnements opérationnels.***
- ***De préciser les attentes relatives à la contribution des sous-traitants et sous-traitants ultérieurs (même si l'exigence de tenue d'un historique des versions est essentielle, mais reste formulée de manière assez générale) ;***

À ce titre, il serait utile d'apporter des éléments complémentaires sur les attentes minimales en matière de gestion des versions, notamment en ce qui concerne les types de modifications à documenter et les déclencheurs de mise à jour ;

- ***En outre, le template n'aborde pas explicitement la contribution des sous-traitants et des sous-traitants ultérieurs à l'AIPD.***

En pratique, les responsables de traitement, notamment dans des environnements complexes, dépendent fortement des sous-traitants pour :

- ***Les informations techniques (architecture, mesures de sécurité) ;***
- ***La description des flux de données ;***
- ***La localisation des traitements.***

Il serait opportun d'intégrer :

- ***Une référence explicite à la contribution attendue des sous-traitants à l'AIPD ;***
- ***Un lien avec les obligations prévues à l'article 28 du RGPD (assistance au responsable de traitement) ;***
- ***Des indications sur la manière de documenter cette contribution.***

- ***Enfin, le template évoque la possibilité de publier l'AIPD, mais sans fournir de lignes directrices détaillées. Il serait utile de préciser le niveau d'information pouvant être partagé en externe. À cet égard, le template repose sur une cohérence implicite avec le registre des traitements (article 30 RGPD), sans en préciser les modalités pratiques. En l'absence de clarification sur la réutilisation des informations existantes, il existe un risque de duplication et de création de silos documentaires. Il pourrait être utile d'encourager explicitement des mécanismes de renvoi et de capitalisation entre le registre et l'AIPD, afin de garantir la continuité et la cohérence de la documentation.***

3. Description « moyens/architecture/actifs » (rubrique 1.3)

Le *template* demande de décrire les moyens de traitement, actifs de support et architecture sous-jacente avec un niveau de détail élevé, ce qui constitue une avancée pour améliorer la qualité des AIPD.

Toutefois, pour des traitements industrialisés (traçabilité colis, plateformes de services, SI RH), il existe un risque de produire une documentation trop technique et difficile à maintenir, alors que l'objectif des AIPD est avant tout la maîtrise des risques et la

justification des mesures.

Dans ce contexte, le niveau de granularité attendu gagnerait à être explicitement précisé et adapté en fonction de la complexité du traitement, du niveau de risque, ainsi que de la taille et de l'organisation de l'entité concernée.

En pratique, certaines informations ont vocation à être intégrées directement dans l'AIPD afin d'en garantir une vision synthétique et intelligible, tandis que d'autres, plus techniques, relèvent de documentations distinctes (notamment IT, sécurité ou architecture), auxquelles l'AIPD peut utilement renvoyer.

Le groupe La Poste propose :

- ***De clarifier, dans le template, le niveau de granularité attendu, en précisant qu'il doit être proportionné à la complexité du traitement et au niveau de risque et du contexte organisationnel (tels que l'architecture logique, les composants critiques et les points de concentration du risque) plutôt qu'un inventaire exhaustif.***
- ***D'introduire une possibilité explicite de référencer des documents déjà existants (PSSI, dossiers d'architecture, analyses de risques SSI) en précisant que l'AIPD peut s'appuyer sur ces éléments, tout en n'en reprenant que les informations nécessaires à l'analyse des risques pour les droits et libertés des personnes.***

4. « Secondary or compatible uses » /réutilisation (rubrique 1.1.3)

Le *template* prévoit d'identifier les usages secondaires ou compatibles. Dans un groupe multiservices, il s'agit d'un enjeu particulièrement structurant, compte tenu de la fréquence des réutilisations de données (référentiels partagés, interconnexions, amélioration continue, *analytics*, lutte contre la fraude, etc.).

L'intégration de cette rubrique dans le *template* traduit l'introduction explicite d'une analyse de compatibilité au sens du RGPD, impliquant d'identifier les réutilisations de données et d'en justifier la compatibilité avec les finalités initiales. Cette exigence a un impact structurant sur les pratiques, en appelant à un encadrement renforcé des logiques de réutilisation.

Toutefois, en pratique, cette rubrique peut être difficile à stabiliser dans le temps, en raison de l'émergence régulière de nouveaux cas d'usage et d'innovations.

Le groupe La Poste recommande :

- ***D'introduire une approche guidée (par exemple sous forme de questions) permettant d'accompagner la mise en œuvre pratique de l'analyse de compatibilité, au titre de l'article 6.4 du RGPD dans le cadre de l'AIPD. À cet effet, les lignes directrices pourraient préciser les éléments d'analyse attendus, notamment :***
  - ***Si l'usage secondaire est prévu dès la conception ou introduit ultérieurement ;***
  - ***Les critères de compatibilité retenus ;***
  - ***Les impacts spécifiques sur les droits et attentes des personnes.***
- ***D'encourager une traçabilité des évolutions associées aux usages secondaires, en lien avec les mécanismes de gestion de versions de l'AIPD, dans la mesure où ces évolutions constituent un point de vigilance particulier en matière de dérives potentielles.***

5. Licéité/bases légales/levées d'interdiction (rubriques 2.1.1 – 2.1.2)

Le *template* intègre utilement l'identification de la base légale applicable ainsi que, le cas échéant, des motifs permettant de lever l'interdiction de traitement pour certaines catégories de données. Cet apport est particulièrement pertinent pour des traitements impliquant des catégories particulières de données ou soumis à des contraintes spécifiques.

Toutefois, le groupe La Poste considère que la formulation actuelle gagnerait à mieux distinguer les situations dans lesquelles les traitements relèvent respectivement :

- D'obligations légales ou réglementaires ;
- De missions d'intérêt général ou de service public ;
- De besoins contractuels liés à la fourniture de services aux clients ;
- Et/ou d'exigences de sécurité, de continuité d'activité ou de prévention de la fraude.

➢ ***Le groupe La Poste propose de clarifier, dans le document explicatif accompagnant le template, l'articulation attendue entre l'analyse de la base légale (rubrique 2.1) et l'évaluation de la nécessité et de la proportionnalité du traitement (rubrique 3), afin d'éviter tout risque de redondance ou de confusion entre l'analyse juridique du fondement du traitement et l'analyse d'impact sur les droits et libertés des personnes concernées.***

6. Mesures de conformité (rubrique 2.3) et « privacy by design/default »

Le *template* impose de démontrer que le traitement envisagé est à la fois efficace et le moins intrusif possible pour les droits et libertés des personnes concernées. Cette exigence constitue un élément central de l'analyse de proportionnalité et un levier essentiel d'*accountability*.

Toutefois, en pratique, la notion de « nécessité » demeure complexe à appréhender et le *template* ne fournit pas de méthodologie suffisamment concrète pour guider cette analyse, en particulier dans des environnements techniques ou organisationnels complexes.

Le groupe La Poste recommande :

➢ ***De préciser les attentes en matière d'évaluation de la nécessité, en intégrant une approche plus opérationnelle de cette analyse, notamment à travers :***
- ***Une comparaison des différentes alternatives possibles ;***
- ***Une justification documentée du choix retenu ;***
- ***Une clarification de la distinction entre « risque de conception » et « risque d'incident », ainsi que de ses implications opérationnelles, en particulier lorsque certains risques ne peuvent être atténués par des mesures techniques mais sont inhérents aux choix de conception du traitement.***

➢ ***D'illustrer cette analyse par des exemples concrets d'alternatives pertinentes, tels que :***
- ***Le recours à l'anonymisation ou à la pseudonymisation ;***
- ***Des mesures de minimisation des données ;***

- ***Des choix d'architecture technique moins intrusifs.***

7. Méthode de risque : risque inhérent/résiduel et plan d'action (rubrique 4)

Le *template* prévoit une section structurée « *risk assessment and management* », incluant méthode, risque inhérent, plan d'action, mesures additionnelles, risque résiduel, fondée sur la combinaison de la probabilité et de la gravité des impacts, selon une approche standard de calcul du risque (« *risk = likelihood × severity* »), ce qui constitue une base méthodologique solide et alignée avec les standards existants.

Toutefois, un point d'attention important réside dans l'interprétation homogène des échelles et des critères entre organisations et autorités de contrôle. En l'absence de critères suffisamment précis pour qualifier la probabilité de survenance des risques et la gravité de leurs impacts sur les droits et libertés des personnes, cette approche est susceptible d'entraîner des appréciations subjectives et des pratiques hétérogènes.

Le groupe La Poste suggère :

- ***D'ajouter des orientations minimales dans l'explainer relatives à l'évaluation des risques, en précisant :***
- ***Les critères permettant d'apprécier de manière plus homogène la probabilité (likelihood) et la gravité (severity) des risques (tels que la nature des données, l'ampleur des impacts, la vulnérabilité des personnes concernées et le contexte du traitement) ;***
- ***Des exemples d'échelles d'évaluation (probabilité/gravité) ou, a minima, recommander que les organisations explicitent leur référentiel interne afin de garantir la comparabilité.***

- ***D'autoriser et d'encourager l'utilisation de bibliothèques de scénarios types (distinguant, notamment, les risques structurels et les risques incidentels) en particulier pour les organisations industrielles, afin de faciliter l'harmonisation des analyses de risques et de réduire les divergences d'interprétation.***

8. « Involvement of interested parties » : avis DPO et vues des personnes (rubrique 5)

Le *template* prévoit l'avis du DPO et les vues des personnes concernées/leurs représentants. Pour les grands groupes et certains traitements « infrastructurels » (SI RH, traçabilité, outils internes, etc.), la collecte de « *views of data subjects* » peut être difficile ou non pertinente au cas par cas.

Le groupe La Poste propose :

- ***De clarifier que cette rubrique peut être satisfaite par (i) des mécanismes existants (représentants du personnel, enquêtes internes, retours clients), ou (ii) une justification motivée lorsque la consultation n'est pas adaptée, afin de préserver une approche proportionnée.***

LA POSTE
GROUPE

9. Consultation préalable de l'autorité de contrôle (rubrique 6)

Le *template* prévoit formellement la possibilité de recourir à une consultation de l'autorité de contrôle, sans toutefois fournir d'orientations opérationnelles suffisantes permettant d'en guider la mise en œuvre.

En pratique, l'absence de critères d'arbitrage clairs est susceptible de générer une incertitude, en particulier pour des traitements complexes, structurants ou relevant de missions d'intérêt général.

Le groupe La Poste recommande :

- ***De préciser les critères permettant d'orienter la décision de recourir ou non à la consultation préalable, en tenant compte par exemple du niveau de risque résiduel, de la nature des traitements et de la sensibilité des données) ;***
- ***De fournir des exemples de cas d'usage ou de situations types, afin de renforcer l'opérationnalité de cette étape.***

Conclusion

Au-delà des observations formulées sur les différentes sections du *template*, plusieurs enjeux transversaux apparaissent.

En particulier, l'articulation avec les dispositifs existants, notamment le registre des traitements (article 30 RGPD), gagnerait à être précisée afin d'éviter toute duplication documentaire et de favoriser une logique de capitalisation.

De même, les modalités de recours à la consultation préalable de l'autorité de contrôle (article 36 RGPD) nécessiteraient des orientations opérationnelles complémentaires afin de guider les responsables de traitement dans leurs décisions.

Enfin, la question de la soutenabilité du modèle dans le temps constitue un enjeu structurant pour les organisations complexes. À cet égard, un renforcement des mécanismes de proportionnalité, de mutualisation et d'articulation avec les référentiels existants apparaît essentiel.

Ces éléments contribuent à souligner l'importance d'un *template* à la fois harmonisé et pleinement opérable dans des environnements multi-acteurs et industrialisés, tout en garantissant une mise en œuvre proportionnée et adaptée à la complexité des traitements.

Dans cette perspective, le groupe La Poste considère que le *template* gagnerait à être renforcé sur ses modalités de mise en œuvre opérationnelle, afin de concilier harmonisation des pratiques et adaptabilité aux contextes organisationnels complexes.

***

Nous contacter

Christelle DEFAYE-GENESTE, Directrice des Affaires Européennes et Douanières, Représentation de La Poste à Bruxelles - christelle.geneste@laposte.fr

Gaëlle KULIG, Responsable des Affaires Européennes Numériques – gaelle.kulig@laposte.fr

Damien LEGOFF, Group Data Protection Officer, damien.legoff@laposte.fr