Union interparlementaire
Pour la démocratie. Pour tous.

Politique et procédures de l'UIP en matière de protection des données personnelles

Octobre 2022

Table des matières

Document en date du : 14 octobre 2022

Approuvé par : le Conseil directeur

Règlements et documents connexes : Code de conduite de l'UIP

Définitions

Consentement : toute indication par laquelle une personne manifeste de façon libre et éclairée son accord au traitement des données personnelles la concernant, par exemple au moyen d'une déclaration écrite, orale ou par le biais d'un acte positif clair.

Données personnelles : toute information se rapportant à une personne physique identifiée ou identifiable (dénommée 'personne concernée'). L'appellation 'personne physique identifiable' désigne une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données personnelles sensibles : données personnelles relevant des aspects les plus privés de la vie d'une personne concernée, par exemple l'origine raciale ou ethnique, les opinions et affiliations politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, l'état de santé (notamment les données médicales, biologiques ou biométriques), la situation financière ou familiale/relationnelle (notamment la situation conjugale, l'orientation ou les préférences sexuelles, la vie sexuelle et les personnes à charge). Les données sensibles incluent également certains documents liés au parcours professionnel des employés de l'UIP, par exemple ceux relatifs à leurs performances et à leur comportement. L'affiliation politique des parlementaires étant de notoriété publique, elle n'est donc pas concernée par la définition des données personnelles sensibles dans le cadre de la présente politique.

Fournisseur : personne, entreprise ou organisation qui propose, par le biais d'un contrat, des travaux, des biens ou des services autres que le conseil.

Personne concernée : personne physique pouvant être identifiée, directement ou indirectement, en particulier par référence à des données personnelles. Parmi les exemples de personnes concernées potentielles, on peut citer : membres du personnel de l'UIP ou membres des organes directeurs de l'UIP, parlementaires, fournisseurs ou toute personne dont les données personnelles font partie des informations collectées par l'une des entités susmentionnées.

Personnel de l'UIP : tous les membres du personnel de l'UIP ainsi que les personnes ayant d'autres types de contrats, notamment les stagiaires, les employés détachés, les consultants et les collaborateurs externes.

Propriétaire d'informations : personne responsable d'informations spécifiques qui assume la fonction de directeur de division dans le cadre de la présente politique, cette personne devant être considérée propriétaire de toutes les informations générées par sa division ou confiées à cette dernière. Les directeurs de division peuvent déléguer leur responsabilité de propriétaire d'informations à une ou des personne(s) au sein de leur division, s'ils le jugent approprié.

Responsable du traitement des données : membre du personnel de l'UIP détenant l'autorité pour superviser la gestion du traitement des données personnelles et en déterminer les finalités.

Secrétariat de l'UIP : le Secrétariat de l'UIP comprend la totalité du personnel de l'Organisation sous la direction du Secrétaire général de l'UIP.

Sous-traitant des données : tout membre du personnel de l'UIP ou toute personne physique ou morale, agence, autorité publique, notamment un partenaire de mise en œuvre ou un tiers chargé du traitement des données personnelles pour le compte du responsable du traitement des données.

Tiers : personne physique ou morale, autorité publique, agence ou organisme autre que la personne concernée, le sous-traitant des données et le Secrétariat de l'UIP (en tant que responsable du traitement des données) et personnes placées sous l'autorité directe du sous-traitant des données et du responsable du traitement des données. Parmi les exemples de tiers, on peut citer : les Parlements membres, les gouvernements nationaux, les organisations internationales gouvernementales et non gouvernementales, et des personnes ou des entités du secteur privé.

Traitement des données : toute opération ou ensemble d'opérations appliquées à des données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison, le blocage, l'effacement ou la destruction. Le terme “traité” signifie que l'acte de traitement a été effectué.

Transfert de données : tout acte rendant des données personnelles accessibles à un tiers, que ce soit sur papier, par des moyens électroniques, par Internet ou par toute autre méthode. “Transférer” des données personnelles signifie effectuer un transfert de ces données.

Violation de données : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, stockées ou ayant fait l'objet d'un traitement quelconque, ou encore l'accès à de telles données.

* * * * *

I Introduction

1. Dans l'exercice de ses activités, le Secrétariat de l'UIP collecte, stocke et traite des données sur les personnes qui interagissent avec l'UIP, notamment les parlementaires, les membres du personnel et d'autres personnes collaborant avec l'Organisation. L'UIP s'engage à respecter la dignité et la vie privée de ces personnes, tout en conciliant ces droits avec sa capacité à accomplir son mandat.

2. Eu égard à ses mandats et objectifs, l'UIP promeut le respect universel des droits de l'homme et des libertés fondamentales, notamment le droit à la vie privée, et comprend l'importance des politiques, stratégies et normes internationales de protection des données en vue d'assurer le respect de ces droits et libertés. Le but de la présente politique est de définir des principes clés en matière de traitement des données personnelles, de souligner les rôles et responsabilités du Secrétariat de l'UIP, de son personnel et, le cas échéant, de tiers. Les lois et politiques de protection des données personnelles sont destinées à mieux protéger les droits de chaque personne à la vie privée, tout en faisant en sorte que des activités légitimes commerciales et de gouvernance puissent être menées en respectant certains paramètres.

II. Champ d'application

3. La présente politique de protection des données définit l'approche de l'UIP en matière de protection de la confidentialité des données. Elle présente les processus suivis par le Secrétariat de l'UIP en vue de s'assurer qu'il peut accomplir son mandat tout en se conformant aux normes internationalement reconnues en matière de protection des données personnelles.

4. Cette politique s'applique à tout le personnel de l'UIP et, le cas échéant, aux tiers qui reçoivent, stockent et/ou traitent des données personnelles (voir définition ci-dessus), et sont liés à toutes les données personnelles reçues, stockées et/ou traitées par le Secrétariat de l'UIP.

III. Principes de protection des données personnelles

5. Le Secrétariat de l'UIP respectera et appliquera les principes suivants en matière de traitement des données personnelles :

A. Traitement loyal et légitime

6. Les données personnelles seront traitées de manière loyale et transparente, et seulement s'il existe une raison légitime d'effectuer ce traitement. Parmi les raisons légitimes :

- intérêt supérieur de la personne concernée ou d'une autre personne,
- garantir la sécurité des personnes,
- permettre au Secrétariat de l'UIP d'accomplir son mandat,
- exécution d'un contrat,
- conformité avec une obligation légale,
- défense de droits en justice.

7. Le Secrétariat de l'UIP prendra toutes les précautions utiles lors du traitement des données personnelles sensibles. Les données personnelles sensibles ne doivent être traitées que si les personnes concernées ont explicitement donné leur accord, sauf dans les cas suivants :

   - si cela est nécessaire pour s'acquitter des obligations et des droits spécifiques du Secrétariat de l'UIP dans le cadre du Statut du personnel et du Règlement du personnel de l'UIP, ou
   - si le traitement s'effectue dans le cadre des intérêts légitimes du Secrétariat de l'UIP, sous réserve que le traitement ne concerne que le personnel de l'UIP ou les personnes régulièrement en contact avec le Secrétariat de l'UIP dans le cadre des besoins de ce dernier, et sous réserve que les données personnelles sensibles ne soient divulguées à un tiers qu'avec le consentement des personnes concernées.

B. Limitation à une finalité spécifique

8. Les données personnelles ne peuvent être traitées que pour une ou plusieurs finalités spécifiques légitimes, et elles ne peuvent pas faire l'objet d'autres traitements incompatibles avec cette ou ces finalité(s). Le Secrétariat de l'UIP peut traiter les données personnelles à des fins autres que celles spécifiées au moment de leur collecte, sous réserve que ces traitements soient compatibles avec les fins initialement prévues. Toutefois, les traitements ultérieurs ne sont pas autorisés si les risques pour la personne concernée sont plus importants que les avantages découlant de ces autres traitements.

C. Minimisation des données

9. Le traitement des données personnelles doit être nécessaire et proportionné par rapport au(x) but(s) poursuivi(s). Les données personnelles traitées doivent donc être adéquates et pertinentes eu égard au but identifié et elles ne doivent pas sortir du cadre de ce but.

D. Précision

10. Les données personnelles doivent être enregistrées aussi précisément que possible et, le cas échéant, être actualisées pour s'assurer qu'elles répondent au(x) but(s) pour lesquels elles sont traitées. Les personnes concernées doivent être informées quant à l'importance de la précision et de l'exhaustivité des informations fournies, notamment lors de l'actualisation de ces informations, le cas échéant. Tout sera raisonnablement fait pour s'assurer que les données personnelles imprécises sont corrigées ou supprimées sans délai injustifié (en tenant compte du ou des but(s) pour lesquels elles sont traitées ainsi que des principes de minimisation des données et de limitation de leur stockage).

E. Limitation du stockage

11. Les données personnelles doivent être conservées dans un format permettant l'identification des personnes concernées, pas plus longtemps que ce qui est nécessaire, pour le ou les but(s) pour lesquels ces données sont traitées. Les données personnelles peuvent être stockées sur des périodes plus longues dans la mesure où elles ne sont traitées qu'à des fins d'archivage dans l'intérêt général, dans un but statistique ou de recherche historique.

F. Assurer la sécurité et la confidentialité

12. Les données personnelles doivent être traitées de façon à leur garantir une sécurité appropriée, notamment la protection contre tout traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, par application de mesures techniques ou organisationnelles appropriées.

IV. Droits des personnes concernées

A. Droit à l'information et à l'accès

13. Toute personne aura le droit de demander des informations sur ses données à caractère personnel. Une personne concernée pourra demander les informations suivantes au Secrétariat de l'UIP :

   - la confirmation que des données à caractère personnel la concernant ont été, sont ou seront traitées ou non,

- des informations sur les données à caractère personnel en cours de traitement, la ou les raisons pour lesquelles ces données sont traitées et tout tiers à qui ces données ont été, sont ou seront transférées ainsi que la période envisagée pendant laquelle les données à caractère personnel seront stockées par ces tiers,
- les informations communiquées à la personne concernée en réponse à sa demande doivent être concises, transparentes, compréhensibles et présentées sous une forme aisément accessible, et formulées en des termes clairs et simples.

14. Le Secrétariat de l'UIP rendra publiques les informations relatives aux droits des personnes concernées d'accéder à leurs données à caractère personnel, de les rectifier, de les transférer et/ou de les supprimer, aux termes de la présente politique, ainsi que les modalités selon lesquelles une telle demande peut être formulée. Dans l'éventualité d'une telle demande émanant d'une personne concernée, les propriétaires d'informations au sein du Secrétariat de l'UIP coopéreront afin de compiler les informations pertinentes dans un délai raisonnable à déterminer et convenu en coordination avec la personne concernée.

15. Le droit des personnes concernées d'accéder aux informations ne s'applique pas ou peut être limité au motif d'un intérêt public important nécessitant que l'accès soit refusé. Ces intérêts peuvent comprendre :

- le respect de la confidentialité, comme celui des lanceurs d'alerte,
- la viabilité des programmes et des plans de travail mis en œuvre dans le cadre du mandat de l'UIP,
- la protection de la confidentialité des opinions et des arguments logiques du personnel de l'UIP qui, en cas de violation, risqueraient de compromettre les opérations de l'UIP et/ou de divulguer les données à caractère personnel dudit personnel,
- la prévention des représailles,
- le maintien des privilèges et des immunités dont bénéficie l'UIP,
- la défense de droits en justice et le respect des obligations légales,
- l'intégrité des procédures d'audit, d'enquête ou judiciaires, et
- les droits et libertés de tiers qui prévalent sur les intérêts de la personne concernée en matière de protection des données.

16. Le Secrétariat de l'UIP peut également limiter le droit à l'accès aux informations des personnes concernées si leurs demandes sont manifestement excessives.

B. Droit de rectification et d'effacement

17. Une personne concernée peut demander la rectification ou l'effacement de données à caractère personnel inexactes, incomplètes, superflues ou excessives, et le Secrétariat de l'UIP doit rectifier ou effacer ces données, le cas échéant, dans les meilleurs délais. Si elles se rapportent à des documents d'archives ou d'autres informations vérifiables, les données peuvent toutefois être conservées sous leur forme initiale.

C. Droit à la portabilité

18. Une personne concernée peut à tout moment demander une copie de ses données à caractère personnel (dans un format facilement accessible) et/ou demander le transfert de ses données du Secrétariat de l'UIP à un autre responsable du traitement.

D. Droit d'opposition

19. Une personne concernée peut s'opposer à tout moment, pour des motifs légitimes et impérieux tenant à sa situation particulière, au traitement de données à caractère personnel la concernant.

20. Une telle opposition sera acceptée si les libertés et droits fondamentaux de la personne concernée l'emportent sur les intérêts légitimes de l'UIP, ou sur l'intérêt public, en matière de traitement. Si une telle objection est acceptée, le Secrétariat de l'UIP ne pourra plus traiter les données personnelles concernées. En cas de différend concernant une opposition, le propriétaire d'informations doit être consulté et la décision définitive sera prise par le Secrétaire général.

V. Procédures de protection des données à caractère personnel

A. Collecte des données auprès des personnes concernées

21. Lors de la collecte de données à caractère personnel directement auprès d'une personne concernée, le Secrétariat de l'UIP informera celle-ci de ce qui suit :

- la ou les finalités spécifiques pour lesquelles les données à caractère personnel ou les catégories de données à caractère personnel seront traitées,
- si ces données à caractère personnel sont destinées à être transférées à un tiers (et à être rendues publiques),
- l'importance pour la personne concernée de fournir des informations précises et complètes, et de mettre à jour de ces informations le cas échéant, et
- l'existence de la présente politique et les moyens par lesquels la personne concernée peut demander des informations ou exercer ses droits conformément à la présente.

22. Dans la mesure du possible, il sera demandé à la personne concernée de reconnaître qu'elle a reçu les informations susmentionnées et qu'en fournissant ses données à caractère personnel, elle consent à la collecte pour des fins déterminées et à leur transfert éventuel, le cas échéant.

B. Fournisseurs

23. Lorsque la collecte et le traitement de données à caractère personnel constituent l'une des responsabilités d'un fournisseur, le Secrétariat de l'UIP veillera à ce que celui-ci s'engage à respecter les principes de base relatifs à la protection des données à caractère personnel, et les normes similaires ou comparables en la matière, énoncés dans cette politique.

C. Confidentialité et sécurité des données personnelles

24. L'UIP classe les données à caractère personnel comme informations confidentielles. Le Secrétariat de l'UIP veille notamment à ce que les données personnelles sensibles soient traitées de manière appropriée afin de préserver leur confidentialité.

25. Les mesures de sécurité des données du Secrétariat de l'UIP sont conçues et mises en œuvre pour protéger les données à caractère personnel contre les risques de destruction, de perte, d'altération, de divulgation non autorisée de données à caractère personnel, ou d'accès non autorisé à de telles données, de manière accidentelle ou illicite. Le Secrétariat de l'UIP garantit la sécurité des systèmes informatiques et des technologies de l'information qui facilitent l'application de cette politique.

D. Garantir l'exactitude des données à caractère personnel

26. Le personnel de l'UIP doit s'assurer que le Secrétariat de l'UIP maintient à jour ses données à caractère personnel, tel que demandé par la Directrice des Services administratifs. Le personnel de l'UIP doit dans les plus brefs délais notifier les changements qui ont été apportés pour garantir en toutes circonstances l'exactitude des données personnelles.

27. Le Secrétariat de l'UIP actualisera s'il y a lieu les données à caractère personnel et les vérifiera régulièrement. Les données à caractère personnel contenues dans ses systèmes devront être effacées si l'on apprend qu'elles sont inexactes, superflues ou excessives. Lorsque cela est possible et approprié, les corrections éventuelles à apporter doivent être confirmées par la personne concernée.

28. Lorsque des données à caractère personnel sont rectifiées ou effacées des systèmes du Secrétariat de l'UIP, étant inexactes, superflues ou excessives, il convient dans la mesure du possible de contacter le tiers auquel ces données pertinentes ont été transmises en tenant compte de facteurs tels que l'objectif initial du transfert, la poursuite ou non de l'objectif visé et la conformité attestée ou non aux principes énoncés dans la présente.

E. Notification d'une violation de données

29. Le personnel de l'UIP est tenu d'aviser dans les plus brefs délais le propriétaire d'informations et le directeur de la communication lorsqu'il aura constaté une violation des données à caractère personnel ou une violation présumée, et d'enregistrer comme il se doit l'infraction. Si des données personnelles sensibles ont été compromises ou pourraient l'avoir été (par exemple une perte, une modification, un accès ou une divulgation, de manière illicite ou accidentelle), cela sera immédiatement signalé.

30. Si une violation de données à caractère personnel peut causer un préjudice personnel à une personne concernée, le propriétaire d'informations mettra tout en œuvre pour communiquer à cette personne la violation de données à caractère personnel et prendra sans plus tarder les mesures d'atténuation appropriées, à moins que :

- cela n'implique des efforts démesurés, en raison de problèmes logistiques ou des conditions de sécurité, ou du nombre de cas concernés. Dans ce cas, le propriétaire d'informations déterminera s'il est opportun de faire une déclaration publique ou de prendre des mesures analogues par lesquelles les personnes concernées sont informées d'une manière raisonnablement susceptible d'être efficace,
- cela ne constitue un manquement à une obligation légale,
- cela ne porte préjudice aux privilèges et immunités dont jouit l'UIP,
- cela ne soit pas nécessaire pour faire valoir ses droits, ou
- l'appréhension des personnes concernées, compte tenu du climat d'insécurité ou de la situation politique, ne les mette en danger ou ne leur cause une grave détresse.

F. Conservation

31. Les données à caractère personnel doivent être conservées aussi longtemps que nécessaire aux fins pour lesquelles elles sont collectées et traitées sans préjudice de la conservation des documents d'archives qui doivent être préservés provisoirement ou définitivement en raison de leur intérêt administratif, budgétaire, juridique, scientifique, historique ou de leur valeur d'information.

VI. Protection des données par des tiers

A. Sur une base contractuelle

32. Si le Secrétariat de l'UIP collabore avec un tiers pour traiter des données à caractère personnel, les responsabilités des deux parties seront définies et précisées dans un contrat établi entre le Secrétariat de l'UIP et cette autre entité afin de permettre au Secrétariat de l'UIP de garantir le respect de la confidentialité, de préciser le ou les finalités spécifiques et la légitimité du traitement des données à caractère personnel, et de veiller à ce que la présente politique soit toujours respectée.

33. Un tiers n'est pas habilité à sous-traiter le traitement des données à caractère personnel à une autre partie, ou de recruter une autre entité, sans autorisation écrite préalable de l'UIP. Tout ajout ou remplacement ultérieur d'un sous-traitant par un tiers doit être effectué dans les mêmes conditions.

34. Quelles que soient les obligations énoncées dans un accord, le Secrétariat de l'UIP vérifiera, avant de transférer des données à caractère personnel à un sous-traitant des données ou d'en recruter un pour traiter ces données, que le traitement des données à caractère personnel par le responsable du traitement satisfait aux principes énoncés dans la présente.

VII. Transfert de données

A. Limites applicables au transfert de données

35. Le Secrétariat de l'UIP peut transférer des données à caractère personnel à un tiers à condition que ce dernier offre un niveau de protection des données similaire ou comparable aux normes énoncées dans la présente politique, et que les personnes concernées ont été informées du transfert possible de leurs données à caractère personnel. En particulier, et sans limitation de ce qui précède, les transferts de données sont soumis aux conditions suivantes :

- le transfert de données doit reposer sur une ou plusieurs bases légitimes,
- le transfert de données doit être effectué à une ou plusieurs fins précises et légitimes,
- le traitement par un tiers doit se limiter autant que possible à une ou plusieurs fins précises,
- la quantité et le type de données à caractère personnel à transférer se limite strictement à la nécessité du tiers de connaître les fins prévues énoncées,
- le transfert de données ne doit pas être incompatible avec les attentes raisonnables de la personne concernée, et
- il faut s'assurer que les droits de la personne concernée sont respectés et que le destinataire a au moins mis en place des mesures appropriées de protection et de contrôle de la divulgation des données, ou des garanties en la matière, et qu'il respecte la confidentialité des données qui sont divulguées par l'UIP, afin de maintenir un niveau approprié de sécurité des données,
- le transfert de données répond aux conditions applicables énoncées dans la section sur les garanties ci-dessous.

36. Dans le cadre des activités qui lui ont été confiées, le Secrétariat de l'UIP peut donner à ses Membres un accès restreint aux données à caractère personnel par le biais du Répertoire de l'UIP. Les Membres s'attacheront à respecter les principes généraux de cette politique et à mettre en place des garanties pour la protection et la sécurité des données qui leur ont été confiées par l'UIP.

B. Transfert de données aux Parlements membres, aux organismes nationaux d'application des lois et aux juridictions nationales

37. Dans certaines circonstances et sans préjudice des privilèges et immunités dont jouit l'UIP, le Secrétariat de l'UIP peut transférer des données à caractère personnel à un Parlement membre, à un organisme national d'application des lois ou à une juridiction nationale. Ces transferts peuvent être réalisés à la propre initiative de l'UIP ou à la demande d'un Parlement membre, d'un organisme national d'application des lois ou d'une juridiction nationale (pouvant avoir un caractère contraignant ou non pour le Secrétariat de l'UIP). Le transfert peut concerner des personnes faisant l'objet d'une enquête pour un crime qui aurait été commis ou une violation des droits de l'homme, ou en lien avec la ou les victimes ou le ou les témoins d'un crime impliquant des dirigeants d'ONG qui pourraient être qualifiés de "victimes" ou de "témoins". Ces transferts qui ne sont pas réalisés à l'initiative de l'UIP nécessiteront l'approbation du Secrétaire général, sur recommandation du propriétaire d'informations.

38. Outre les conditions générales applicables au transfert de données à caractère personnel à des tiers, l'UIP se pliera à cette demande et transférera des données à caractère personnel à un Parlement membre, à un organisme national d'application des lois ou à une juridiction nationale uniquement si les conditions suivantes sont remplies :

    i. le transfert est nécessaire à des fins de détection et de prévention d'une grave infraction pénale, d'enquête ou de poursuites en la matière, portant atteinte à la sécurité d'un individu ou du public,

    ii. la compétence du demandeur s'étend à la prévention et la détection des infractions en question, ainsi qu'aux enquêtes et poursuites en la matière,

    iii. le transfert aidera considérablement le demandeur dans la poursuite de ces objectifs et ces données à caractère personnel ne pourraient être obtenues à partir d'autres sources,

    iv. le transfert ne porte pas atteinte de façon disproportionnée au droit à la vie privée ou à d'autres droits de l'homme d'une personne concernée ou d'une quelconque autre personne,

    v. dans le cas de données concernant les victimes et les témoins, leur consentement au transfert a été obtenu,

vi. avant de transférer les données à caractère personnel au demandeur, il convient de demander l'avis du délégué à la protection des données après avoir consulté le conseiller juridique et le directeur de la division concernée.

C. Garanties

39. Afin de veiller au respect des principes susmentionnés, des garanties appropriées doivent être fournies, à savoir :

- Le Secrétariat de l'UIP doit assurer la mise en œuvre des garanties et procédures organisationnelles, administratives, physiques et techniques appropriées afin d'assurer la sécurité des données à caractère personnel traitées par l'UIP, notamment contre tout accès, dommage, perte ou autre risque, illicite ou accidentel, inhérent au traitement de données à caractère personnel (violations de données).

- Les faits concernant la violation présumée ou réelle de données doivent être notifiés dès que possible à la personne concernée. Il convient d'évaluer leur gravité et de prendre sans tarder des mesures appropriées destinées à protéger les personnes concernées affectées, notamment pour atténuer ou pallier les répercussions possibles, conformément aux procédures internes.

- Eu égard aux technologies disponibles, les garanties et procédures doivent être raisonnables et adaptées aux risques liés à la nature et au traitement des données à caractère personnel et leur niveau de confidentialité.

40. À moins que des raisons valables ne s'y opposent, avant de transférer des données à caractère personnel à un tiers, le responsable du traitement doit chercher à conclure un accord de transfert de données ou, le cas échéant, à introduire des dispositions relatives à la protection des données dans des accords plus larges, en particulier lorsque les transferts de données à caractère personnel seront vraisemblablement importants, répétés ou structurels, c'est-à-dire lorsque des données du même type sont partagées avec le même tiers aux mêmes fins pendant une certaine période.

41. Les accords de transfert de données doivent, entre autres :

i) préciser la ou les raisons pour lesquelles les données sont transférées, les éléments de données spécifiques à transférer ainsi que les mesures de protection et de sécurité des données à mettre en place,
ii) exiger d'un tiers qu'il veille à ce que ses mesures de protection et de sécurité des données respectent la présente politique, et
iii) préciser les mécanismes de consultation, de supervision, de responsabilité et d'examen pour le contrôle du transfert réalisé en vertu de l'accord.

42. Le responsable du traitement et le conseiller juridique de l'UIP doivent examiner tous les accords de transfert de données.

43. Si tout est mis en œuvre pour s'assurer que les garanties susmentionnées sont respectées en cas de transfert de données à caractère personnel, les autres motifs possibles de transfert de données à caractère personnel comprennent :

- la réalisation des objectifs et l'accomplissement du mandat de l'UIP,
- le consentement de la personne concernée,
- les intérêts vitaux ou impérieux des personnes concernées ou d'autres personnes,
- l'intérêt public, en fonction du mandat de l'UIP,
- la sécurité des personnes,
- l'exécution d'un contrat entre le Secrétariat de l'UIP et la personne concernée, ou
- la défense de droits en justice ou le respect d'obligations légales.

44. L'UIP peut recevoir des données à caractère personnel de tiers (données entrantes) :

- dans le cas où l'UIP collabore avec des tiers afin de recueillir des données à caractère personnel au nom de l'UIP, ceux-ci devront offrir un niveau de sécurité et de protection approprié des données à caractère personnel à la lumière des principes de la présente politique lors de la collecte de données à caractère personnel,

- dans le cas où elle reçoit des données à caractère personnel de tiers n'agissant pas en son nom, l'UIP doit prendre des mesures raisonnables et proportionnées pour s'assurer que ces données à caractère personnel ont été recueillies légalement.

VIII. Transparence

45. Dans la mesure où les objectifs spécifiés pour lesquels sont traitées les données à caractère personnel ne sont pas compromis, l'UIP doit traiter ces données en toute transparence, au besoin et dans la mesure du possible, en communiquant aux personnes concernées des informations sur le traitement de leurs données à caractère personnel selon les conditions spécifiées dans cette politique, notamment si les données à caractère personnel peuvent être transférées à des tiers, et des précisions sur la façon de demander l'accès, la vérification, la rectification et/ou l'effacement de leurs données à caractère personnel.

46. Lorsque ces demandes sont manifestement abusives, frauduleuses ou trop onéreuses pour s'y conformer compte tenu des ressources existantes, l'UIP refusera généralement d'y répondre.

IX. Redevabilité

47. Pour garantir l'imputabilité du traitement de données à caractère personnel et veiller à l'application adéquate de la présente politique, le responsable du traitement est tenu de mettre en œuvre et de superviser le traitement des données à caractère personnel relevant de sa responsabilité. Il lui incombe donc en premier lieu de veiller à ce que la politique soit respectée.

48. Le Secrétaire général peut mettre en place davantage de procédures, normes, directives et séances de formation, ainsi qu'une structure de gouvernance appropriée pour superviser le traitement des données à caractère personnel, et des mécanismes de recours pour traiter les demandes et les réclamations des personnes concernées.

49. L'UIP nomme du personnel chargé de mettre en œuvre et de contrôler les mesures et procédures de sécurité informatique.

50. Le Secrétariat de l'UIP et les Parlements membres prennent toutes les mesures envisageables et veillent au respect des principes énoncés dans la présente politique lorsqu'ils traitent des informations confidentielles et des données personnelles sensibles émanant de l'UIP ou communiquées aux Parlements membres, et s'engagent à en préserver la confidentialité. Le non-respect de ces obligations peut faire l'objet de mesures disciplinaires ou, le cas échéant, de poursuites judiciaires et/ou de mesures correctives.

X. Privilèges et immunités

51. Le respect et l'application de la présente politique par l'UIP n'affectent pas les privilèges et immunités dont jouit l'UIP. Plus particulièrement, le traitement des données à caractère personnel ou, pour le compte de l'UIP, ne sera en aucun cas réputé constituer :

    i) l'acceptation de l'applicabilité des dispositions législatives ou réglementaires au niveau national, régional ou international, ou

    ii) l'acceptation des compétences et pouvoirs des juridictions ou des organismes, ou de toute autre autorité, eu égard aux activités de traitement des données menées par ou au nom de l'UIP.

[fin de la politique]