COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 7 septembre 2018 T-PD(2018)18 Final

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

GUIDE DES PRINCIPES EN MATIÈRE DE RESPECT DE LA VIE PRIVÉE ET DE PROTECTION DES DONNÉES AUX FINS DU TRAITEMENT DE DONNÉES EN LIEN AVEC L'ICANN

Direction générale des droits de l'Homme et de l'État de droit

Le présent guide est destiné[1] à faciliter l'intégration et l'observation de principes internationalement reconnus en matière de respect de la vie privée et de protection des données.

1. Définitions (voir l'Annexe)

Tout d'abord, il est de la plus haute importance que les principaux concepts et définitions relatifs au respect de la vie privée et à la protection des données soient communément compris. Bien qu'il puisse exister des différences minimes dans certains pays, les données à caractère personnel s'entendent de toute information concernant une personne physique identifiée ou identifiable. On notera que dans la plupart des pays, les données se rapportant aux personnes morales ne sont pas considérées comme des données à caractère personnel, sauf si elles permettent l'identification d'une personne physique. Dans un contexte ICANN, même d'insignifiantes données WHOIS, adresses IP (adresses dynamiques comprises), métadonnées, etc. doivent être considérées comme des données à caractère personnel, car il est possible d'identifier une personne physique en utilisant ces données ou en les associant à d'autres données publiquement et aisément accessibles.

Pour ce qui est du traitement de données, il convient de noter que chaque action portant sur des données à caractère personnel, même si elle fait partie d'une opération technique complexe, ou lorsqu'elle correspond à la tenue d'un registre public ou au dépôt fiduciaire ('*escrow*') de ces données, est considérée comme un traitement.

Pour définir qui est le responsable du traitement dans le réseau d'opérations extrêmement complexe de l'ICANN, il faut s'intéresser au niveau ou à la localisation dans le système du pouvoir de décision relatif au traitement des données. Pour ce qui est des actions spécifiques effectuées sur les données (pendant les opérations courantes), celui qui prend les décisions clés concernant le traitement de données (par exemple, celui qui détermine les motifs justifiant le traitement, ses finalités et les moyens utilisés et qui contrôle les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder) est qualifié de responsable du traitement. Si l'on s'intéresse de plus près à ce pouvoir de décision, on peut démontrer dans certains cas qu'il existe non seulement une mais deux ou plusieurs organisations qui disposent d'un pouvoir de décision, en tant que coresponsables. À ce titre, elles assument la responsabilité commune et partagée du traitement des données.

2. Principe de la spécification des finalités

Conformément au principe de la spécification des finalités, les données à caractère personnel sont uniquement traitées pour des finalités explicites, déterminées et légitimes et ne sont pas traitées de manière incompatible avec ces finalités. On notera que les responsables du traitement disposent de différents outils pour respecter ce principe.

Pour contribuer à un niveau élevé de responsabilité, les responsables du traitement sont encouragés à définir, avant tout traitement de données, une déclaration de finalités claire. Il y a lieu de se demander pourquoi l'organisation traite des données à caractère personnel. Dans le contexte de l'ICANN, cela impliquerait au moins deux déclarations de finalités liées aux données des titulaires : l'une concernant la politique de l'ICANN selon laquelle les données sont traitées, et l'autre pour la partie contractante qui conclura un contrat avec la personne concernée, le titulaire. La déclaration de finalités doit être établie par le responsable du traitement et, en cas de coresponsabilité, les responsables, qu'ils soient deux ou plusieurs, doivent s'entendre pour savoir qui traite les données pour quelles finalités et dans quelle mesure.

Une déclaration de finalités peut contenir tous les motifs légitimes pour lesquels une organisation traiterait des données à caractère personnel. Une certaine prudence s'impose pour dresser la liste de ces finalités, car un responsable du traitement est (et pourrait être) tenu pour responsable de tous les traitements de données qu'il effectue selon cette déclaration de finalités. En outre, si les données sont traitées pour des finalités qui ne figurent pas dans la déclaration, dans la plupart des cas, cela signifie que le traitement est sans finalité, et donc illicite. Une déclaration de finalités peut être modifiée ou ajustée au fil du temps, mais d'une façon

[1] Conformément au paragraphe 9 de la Déclaration du Comité des Ministres du Conseil de l'Europe sur l'ICANN, les droits de l'homme et l'État de droit (3 juin 2015).

générale, elle doit être conforme à la mission, aux pouvoirs, au mandat et au plan de développement de l'organisation. Elle ne doit pas être très longue, mais elle doit toujours contenir d'une manière relativement détaillée toutes les finalités légitimes pour lesquelles l'organisation souhaite traiter les données, y compris toutes les utilisation(s) et réutilisation(s) possibles après la collecte.

En conclusion, une organisation doit définir sa propre déclaration de finalités et ne doit pas traiter les données à caractère personnel qui n'entrent pas dans le cadre de ces finalités (même si les données sont connues ou susceptibles d'être utiles à d'autres organisations).

3. Traitement des données à caractère personnel

Une fois la déclaration de finalités définie, il est conseillé de cartographier toutes les activités de traitement de données que l'organisation entreprendra pendant ses opérations, en précisant le fondement juridique de chaque opération, ainsi que toutes les données à caractère personnel possibles qui seront nécessaires pour ces opérations. Pour finaliser la cartographie, il y a lieu de procéder à un dernier ajustement des trois éléments (traitement des données – fondement juridique – données à caractère personnel) selon la déclaration de finalités prédéfinie afin de conserver uniquement les données qui sont pertinentes et proportionnées.

Si, par exemple, la finalité du traitement de données est la gestion du système de noms de domaine, qui implique un ensemble complexe d'opérations, il est extrêmement important que le responsable prédéfinisse quelles sont les données à caractère personnel qu'il traitera aux différents stades de ses opérations, sur quelle base et pour quel motif. Il sera ainsi plus facile d'évaluer pourquoi il serait nécessaire de traiter, par exemple, l'adresse physique d'un titulaire et pour quelles opérations et quels motifs le responsable utiliserait ces données spécifiques.

Il convient de noter que dans toute législation internationale et nationale dans ce domaine, des exceptions sont prévues qui permettent de limiter les droits au respect de la vie privée et à la protection des données. Ces exceptions concernent habituellement des cas où les données à caractère personnel sont traitées à des fins de sécurité nationale, de défense, de sécurité publique et/ou d'application des lois ou lorsqu'une telle limitation est nécessaire pour protéger la personne concernée ou les droits et libertés fondamentales de tierces personnes, en particulier la liberté d'expression. On notera néanmoins que cela ne signifie pas que les données à caractère personnel puissent être traitées pour ces finalités sans limitation ou que ces finalités puissent être « librement » ajoutées à la déclaration de finalités, mais plutôt que, si la loi prévoit de telles exceptions dans certains cas particuliers, le responsable du traitement peut appliquer des règles différentes au traitement de ces données pour ces finalités. Il faut souligner que les autorités compétentes, comme les autorités répressives, peuvent avoir accès aux données à caractère personnel contenues dans des registres publics ou privés en vertu de procédures légales et conformément au droit interne et international applicable lorsque l'intérêt général est en jeu (maintien de l'ordre public ou prévention, enquêtes et poursuites en matière d'infractions pénales et exécution de sanctions pénales).

Traitement de données : en règle générale, tous les traitements de données doivent respecter les principes de nécessité, de proportionnalité et de limitation des finalités. Cela implique que préexistent des finalités claires et légitimes et que le traitement soit nécessaire et proportionné à ces finalités légitimes. Le traitement de données doit de plus être effectué licitement, loyalement et de manière transparente. L'utilisation ultérieure des données est considérée comme une nouvelle activité de traitement de données ; les mêmes mesures et conditions s'appliquent donc également à ce type de traitement. Les responsables du traitement prennent les mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, ainsi que leur destruction, perte, utilisation, modification ou divulgation accidentelle ou non autorisée. Le responsable du traitement prend note des violations de données qui sont susceptibles de porter gravement atteinte aux droits et libertés fondamentales des titulaires ou autres personnes concernées et en informe l'organisme national compétent (par exemple, l'autorité de contrôle chargée de faire appliquer la loi sur la protection des données dans le pays), voire les personnes concernées elles-mêmes lorsque la violation risque de les exposer à un risque important.

Fondement juridique : il y a lieu de noter que le traitement effectué sur la base du consentement libre, spécifique, éclairé et non équivoque n'est que l'un des fondements juridiques possibles autorisant un responsable à traiter des données à caractère personnel. Il semble que, dans l'environnement de l'ICANN, le traitement des données sur la base du consentement puisse poser problème : en effet, le consentement est

présumé ne pas avoir été donné librement s'il est impossible de donner un consentement distinct pour des opérations différentes de traitement de données à caractère personnel. Il serait donc utile de réfléchir, pour le traitement des données à caractère personnel, à des fondements juridiques qui conviennent mieux au contexte de l'ICANN.

Données à caractère personnel : les données à caractère personnel traitées doivent être exactes et mises à jour pour que la qualité des données soit la plus élevée possible et être conservées en toute sécurité pendant une durée n'excédant pas celle nécessaire à la finalité légitime poursuivie. Les données doivent en outre être adéquates, pertinentes et non excessives au regard des finalités du traitement. En cas de traitement de catégories particulières de données (« données sensibles »), il convient de noter que la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la Convention 108 modernisée)[2], exige qu'une attention et une protection supplémentaires soient accordées, sous la forme de garanties appropriées, au traitement de ces données.

4. Transparence

La transparence est une prescription essentielle imposée à un responsable du traitement en lien avec ses activités de traitement de données. Elle implique qu'il communique aux personnes concernées des informations suffisantes – si aucune exception ou dérogation ne s'applique – concernant le traitement des activités qu'il entreprendra pendant ses opérations, c'est-à-dire avant qu'il ne commence le traitement (droit à l'information des personnes concernées). En outre, des informations détaillées doivent être rendues accessibles aux personnes concernées quant aux activités de traitement des données et à la manière dont elles peuvent exercer leurs droits.

Pour l'ICANN, cette prescription pourrait être respectée en créant un espace web dédié permettant de trouver, d'une manière qui soit facile à comprendre, toutes les informations sur les traitements de données effectués par l'ICANN et donnant aux personnes concernées la possibilité de contacter l'ICANN pour exercer leurs droits, ainsi que les explications requises à cette fin. Ces ressources devraient être accessibles en plusieurs langues.

5. Droits des personnes concernées

D'une manière générale, les personnes concernées doivent pouvoir contrôler leurs données à caractère personnel, ce qui signifie que le traitement des données doit être conforme à la volonté de la personne concernée. Cela implique que la personne concernée doit être convenablement informée de ce qu'il adviendra de ses données et qu'elle doit se voir accorder des droits spécifiques pour conserver le contrôle des données. Ces droits s'appliquent pendant la totalité du cycle de vie des données, quel que soit le nombre des actions de traitement de données ou des responsables du traitement qui traitent les données. Les droits qui peuvent être exercés à tout moment – si aucune exception ou dérogation ne s'applique – conformément à l'article 9 de la Convention 108 modernisée sont le droit d'accès, le droit de ne pas être soumis à une décision affectant la personne concernée de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte, le droit d'opposition, le droit d'effacement, le droit de rectification et le droit de disposer d'un recours. D'autres droits peuvent exister dans certains pays, notamment le droit de blocage, le droit à la portabilité, le droit de connaître le raisonnement qui sous-tend le traitement, le droit de déréférencement et le droit à l'oubli.

Dans un contexte ICANN, un organigramme détaillé des opérations de traitement de données devra être porté à l'attention des personnes concernées par l'ICANN et par les parties contractantes. De plus, il est vivement recommandé de mettre en place une procédure ou un mécanisme aisément accessible permettant aux personnes concernées d'exercer leurs droits sans frais et sans délai excessifs dans des cas particuliers (comme un formulaire de demande d'accès et des coordonnées multilingues, ou les recours disponibles).

[2] Convention 108 modifiée par le Protocole n° STCE [223] : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0

6. Conservation des données

La conservation des données vise à atteindre la finalité du traitement. Les données étant toujours collectées pour une finalité déterminée, il est logique de les conserver uniquement tant que cela sert cette finalité. Les données qui ne servent plus cette finalité doivent être définitivement effacées.

Dans le contexte de l'ICANN, il serait souhaitable d'élaborer à l'échelle de l'organisation une politique de conservation des données (mécanisme de suppression et de conservation indiquant la durée maximale d'enregistrement pour une finalité donnée) contenant aussi un mécanisme de contrôle permettant de vérifier si les données enregistrées servent encore la finalité pour laquelle elles ont été collectées. Les parties contractantes doivent suivre leur politique de conservation des données conformément à la loi applicable.

7. Transfert transfrontière de données

Des données ne devraient être transférées vers un autre pays que si un niveau approprié de protection est garanti. Les moyens permettant de garantir un tel niveau peuvent varier ; il peut s'agir de la loi de l'État auquel les données sont transférées, incluant les traités et accords internationaux en vigueur, ou de garanties *ad ho*c ou standardisées agréées, établies par des instruments juridiquement contraignants et opposables. Des exceptions peuvent s'appliquer, mais elles doivent être interprétées de façon restrictive et dans des cas particuliers.

L'ICANN, en tant qu'organisation mondiale, devrait disposer de sa propre politique de transfert de données. Les règles et/ou régimes applicables au transfert transfrontière de données dépendront en grande partie des relations contractuelles que l'ICANN a et aura avec ses parties contractantes, qui sont ou seront créées selon le cadre juridique national et international applicable. L'ICANN devrait utiliser des garanties *ad hoc* ou standardisées qui puissent être utilisées par l'organisation elle-même pour les flux transfrontières de données mais aussi par les parties contractantes, quelle que soit leur situation géographique.

8. Responsabilité

Les responsables du traitement assument la responsabilité des traitements de données qu'ils effectuent, ce qui signifie qu'ils exercent leur activité conformément à la législation en vigueur. Cette conformité doit pouvoir être démontrée à tout moment et pour toute activité de traitement de données concernant des données à caractère personnel. Cela implique notamment que les responsables du traitement prennent toutes les mesures appropriées pour se conformer aux principes en matière de respect de la vie privée et de protection des données décrits dans le présent Guide et pour être en mesure de démontrer cette conformité, par exemple en utilisant la déclaration de finalités au regard de la conformité au principe de la spécification des finalités.

L'une des mesures qui pourraient être prises pour faciliter la démonstration de la conformité aux prescriptions relatives au respect de la vie privée et à la protection des données serait de désigner un « délégué à la protection des données » disposant des moyens nécessaires à l'accomplissement de son mandat.

De plus, en cas d'élaboration de politiques internes pouvant aboutir, après un examen attentif, à des traitements de données susceptibles de présenter un risque d'atteinte aux droits et libertés des personnes physiques (par exemple, un risque élevé de violation des droits d'une personne concernée au respect de la vie privée et/ou à la protection des données), il est recommandé, afin de prévenir ou de minimiser le risque d'atteinte à ces droits et libertés fondamentales, de procéder à une analyse d'impact et d'élaborer des politiques spécifiquement consacrées à la vie privée pour différents types de traitement de données.

9. Respect de la vie privée dès la conception et respect de la vie privée par défaut

Pour mieux garantir un niveau efficace de protection, les responsables du traitement devraient évaluer l'effet probable du traitement des données à caractère personnel sur les droits et libertés des personnes concernées avant de débuter le traitement. De plus, ils sont tenus de concevoir le traitement de données de façon à minimiser le risque d'atteinte à ces droits et libertés, en s'assurant que les exigences en matière de

protection des données et la protection des droits des personnes concernées sont intégrées dès que possible – soit, dans l'idéal, au stade de la conception de l'architecture et du système – dans les opérations de traitement des données à travers des mesures techniques et organisationnelles.

L'ICANN devrait élaborer des recommandations destinées à renforcer l'application de ces principes dans ses processus décisionnels et internes.

ANNEXE

Aux fins du présent Guide :

a. « traitement de données » s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données ;

b. « responsable du traitement » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres (« coresponsable ») dispose du pouvoir de décision à l'égard du traitement de données ;

c. « données à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;

d. « destinataire » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles ;

e. « catégories particulières de données » signifie les données génétiques ; les données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes ; les données biométriques identifiant un individu de façon unique ; les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle.