ICANN | GNSO

Organisation de soutien aux extensions génériques

Rapport final du processus accéléré d'élaboration de politiques concernant l'étape 2 du travail sur la spécification temporaire relative aux données d'enregistrement des gTLD

31 juillet 2017

Statut du présent document

Ce document constitue le rapport final des recommandations de l'équipe de la GNSO consacrée au processus accéléré d'élaboration de politiques (EPDP) sur l'étape 2 de la spécification temporaire relative aux données d'enregistrement des gTLD, préparé à l'intention du conseil de la GNSO.

Avant-propos

L'objectif du présent rapport final est de documenter les éléments suivants de l'équipe de l'EPDP : (i) les délibérations sur les questions de la charte, (ii) les contributions reçues sur le rapport initial de l'étape 2 de l'EPDP et leur analyse subséquente par l'équipe responsable de l'EPDP, (iii) les recommandations de politiques ainsi que les niveaux de consensus y associés, et (iv) les orientations de mise en œuvre, pour examen par le conseil de la GNSO.

Table des matières

Ce document a été traduit dans plusieurs langues dans un but purement informatif. Le texte original faisant foi (en anglais) peut être consulté sur : https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

1 Résumé analytique

1.1 Contexte

Le 17 mai 2018, le Conseil d'administration de l'ICANN (Conseil de l'ICANN) a adopté la spécification temporaire relative aux données d'enregistrement des domaines génériques de premier niveau (gTLD) (« Spécification temporaire »). La Spécification temporaire apporte des modifications aux exigences existantes des contrats d'accréditation de bureaux d'enregistrement et d'opérateurs de registre afin de les rendre compatibles avec le Règlement général sur la protection des données (RGPD) de l'Union européenne.[1] Conformément aux statuts constitutifs de l'ICANN, la Spécification temporaire prendra fin le 25 mai 2019.

Le 19 juillet 2018, le conseil de la GNSO a lancé un processus accéléré d'élaboration de politiques (EPDP) et a formé l'équipe responsable de l'EPDP consacrée à la spécification temporaire relative aux données d'enregistrement des gTLD. Conformément à la charte, l'adhésion à l'équipe responsable de l'EPDP était expressément limitée. Cependant, l'ensemble des groupes de parties prenantes, des unités constitutives et des organisations de soutien de l'ICANN est représenté au sein de l'équipe responsable de l'EPDP.

Au cours de l'étape 1 de son travail, il a été demandé à l'EPDP de déterminer si la spécification temporaire relative aux données d'enregistrement des gTLD devrait devenir une politique de consensus de l'ICANN tel quel ou avec des modifications. Le présent rapport final concerne l'étape 2 de la charte de l'équipe responsable de l'EPDP, qui comprend : (i) la discussion sur un système normalisé d'accès et de divulgation des données d'enregistrement non-publiques, (ii) les questions citées dans l'annexe de la spécification temporaire relative aux données d'enregistrement des gTLD (« Questions importantes nécessitant des mesures de la part de la communauté »), et (iii) les questions en suspens reportées de l'étape 1, par exemple, les personnes physiques et les personnes morales, l'expurgation du champ « ville », etc. Pour de plus amples renseignements, veuillez consulter ici.

Afin d'organiser son travail, l'équipe responsable de l'EPDP a accordé de diviser son travail en deux ensembles de priorités : priorité 1 et priorité 2. La priorité 1 comprend le SSAD et toutes les questions directement liées. La priorité 2 comprend les questions suivantes :

[1] Le RGPD est disponible sur https://eur-lex.europa.eu/eli/reg/2016/679/oj ; pour avoir des informations sur le RGPD veuillez consulter https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/.

- L'affichage d'information des sociétés affiliées versus les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire accrédités ;
- La distinction entre personnes morales et personnes physiques ;
- L'expurgation du champ « ville »
- La conservation de données
- L'objectif potentiel du bureau du directeur de la technologie de l'ICANN
- La possibilité pour les contacts uniques d'avoir une adresse e-mail anonymisée uniforme
- L'exactitude et le système de signalement de problèmes liés à l'exactitude du WHOIS

L'équipe responsable de l'EPDP a convenu que la priorité devrait être accordée à l'achèvement des délibérations pour les points de priorité 1. Il est toutefois convenu que, dans la mesure du possible, l'équipe s'efforcera également de faire des progrès, parallèlement, sur les points de priorité 2.

1.2 Rapport initial et supplément au rapport initial

Le 7 février 2020, l'équipe responsable de l'EPDP a publié son rapport initial pour consultation publique. Le rapport initial a décrit les questions fondamentales discutées en relation avec le système normalisé d'accès et de divulgation proposé pour les données d'enregistrement des gTLD non publiques (« SSAD ») et les recommandations préliminaires qui l'accompagnent.

Le 26 mars 2020, l'équipe responsable de l'EPDP a publié un supplément à son rapport initial pour consultation publique. Ce supplément concerne les recommandations et/ou les conclusions préliminaires de l'équipe responsable de l'EPDP sur les questions de priorité 2 répertoriées ci-dessus.

À la suite de la publication du rapport initial et du supplément au rapport initial, l'équipe responsable de l'EPDP : (i) a continué à demander des conseils sur les questions juridiques, (ii) a examiné attentivement les commentaires publics reçus en réponse à la publication du rapport initial et de son supplément, (iii) a poursuivi l'examen du travail en cours avec les groupes de la communauté que les membres de l'équipe représentent, (iv) a poursuivi ses délibérations pour la production du présent rapport final qui sera examiné par le conseil de la GNSO et, au cas où il serait approuvé, sera transmis au Conseil d'administration de l'ICANN pour approbation en tant que politique de consensus de l'ICANN. Comme requis par les lignes directrices des groupes de travail de la GNSO, le président de l'équipe responsable de l'EPDP a effectué des appels à consensus sur les recommandations contenues dans le présent rapport final, tel que décrit à l'annexe D. À savoir :

- Onze (11) recommandations ont obtenu la désignation de consensus complet (1, 2, 3, 4, 11, 13, 15, 16, 17, 19 et 21)

- Trois (3) recommandations ont obtenu la désignation de consensus (7, 20 et 21)
- Six (6) recommandations ont fait l'objet d'un fort soutien mais avec des objections considérables (5, 8, 9, 10, 12 et 18)
- Deux (2) recommandations ont été signalées comme faisant l'objet de divergences (6 et 14)

Pour de plus amples détails sur ces désignations, veuillez consulter l'article 3.6 des Directives de la GNSO pour les groupes de travail.

Recommandations pour examen par le conseil de la GNSO (consulter le chapitre 3 pour voir le texte intégral des recommandations) :

Recommandations du SSAD :

Recommendation 1	**Accréditation**
Recommendation 2	**Accréditation des entités gouvernementales**
Recommendation 3	**Critères et contenu des demandes**
Recommendation 4	**Accusé de réception**
Recommendation 5	**Exigences de réponse**
Recommendation 6	**Niveaux de priorité**
Recommendation 7	**Objectifs du demandeur**
Recommendation 8	**Autorisation des parties contractantes**
Recommendation 9	**Automatisation du traitement SSAD**
Recommendation 10	**Détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD**
Recommendation 11	**Termes et conditions du SSAD**
Recommendation 12	**Obligation de divulgation**
Recommendation 13	**Politique applicable aux requêtes**
Recommendation 14	**Viabilité financière**
Recommendation 15	**Journalisation**

Recommendation 16 **Audits**

Recommendation 17 **Exigences concernant les rapports**

Recommendation 18 **Révision de la mise en œuvre des recommandations de politiques concernant le SSAD à l'aide d'un comité permanent de la GNSO**

Recommandations de priorité 2 :

Recommendation 19 **Affichage de l'information des sociétés affiliées et/ou des fournisseurs des services d'anonymisation et d'enregistrement fiduciaire accrédités ;**

Recommendation 20 **Champ ville**

Recommendation 21 **Conservation des données**

Recommendation 22 **Finalité 2**

Conclusions de priorité 2 :

Conclusion Nº 1. **Finalité de l'OCTO**

Conclusion Nº 2. **Exactitude et système de signalement de problèmes liés à l'exactitude du WHOIS**

En raison des dépendances externes et des contraintes temporelles, le présent rapport final n'aborde pas tous les points de priorité 2. Plus précisément, les éléments suivants ne sont pas traités :

La distinction entre personnes physiques et personnes morales : bien que la question ait été examinée à l'étape 2, cela n'a pas donné lieu à un accord sur les nouvelles recommandations de politique. L'étude demandée sur ce sujet a été reçue trop tard dans le processus pour être dûment prise en considération. Par conséquent, en vertu des recommandations de l'étape 1 de l'équipe responsable de l'EPDP les bureaux d'enregistrement et les opérateurs de registre sont autorisés à différencier entre les enregistrements de personnes physiques et morales sans, toutefois, être tenus de le faire. D'autres travaux sur cette question (y compris l'examen de la différenciation de l'ICANN entre les personnes morales et les personnes physiques dans l'étude des services d'annuaire de données d'enregistrement de noms de domaine (RDDS)) sont en cours d'examen par le conseil de la GNSO.

Faisabilité d'une adresse e-mail anonymisée uniforme pour les contacts uniques : L'équipe responsable de l'EPDP a reçu des directives juridiques indiquant que la publication d'adresses e-mail anonymes uniformes entraîne la publication de données

à caractère personnel ; ce qui montre qu'il peut ne pas être possible de publier une grande échelle d'adresses e-mail anonymes uniformes aux termes du RGPD. D'autres travaux sur cette question sont en cours d'examen par le conseil de la GNSO.

L'équipe responsable de l'EPDP consultera le conseil de la GNSO sur la façon de traiter les autres points de priorité 2.

1.3 Conclusions et prochaines étapes

Ce rapport final sera présenté au conseil de la GNSO à des fins d'examen et d'approbation.

1.4 Autres parties importantes de ce rapport

Pour un examen complet des questions et des échanges pertinents de cette équipe responsable de l'EPDP, les parties suivantes sont comprises dans le présent rapport final :

- Le contexte des questions à l'examen ;
- La documentation concernant les participants aux délibérations de l'équipe responsable de l'EPDP, les registres d'assistance et les liens vers les manifestations d'intérêt, le cas échéant ;
- Une annexe comprenant la mission de l'équipe responsable de l'EPDP comme définie dans la charte que le conseil de la GNSO a adoptée ; et
- Les documents concernant la demande de commentaires de la part de la communauté par le biais des canaux formels des SO/AC/SG/C, y compris leurs réponses.

2 Approche de l'équipe responsable de l'EPDP

La présente section donne un aperçu de la méthodologie de travail et de l'approche de l'équipe responsable de l'EPDP. Les points décrits ci-dessous visent à fournir au lecteur les informations de contexte pertinentes sur les processus et les délibérations de l'équipe responsable de l'EPDP et ne devraient pas être interprétés comme représentant la totalité des délibérations du groupe de travail.

2.1 Méthode de travail

L'équipe responsable de l'EPDP a commencé ses délibérations sur l'étape 2 le 2 mai 2019. L'équipe a accordé de continuer son travail principalement à travers des conférences téléphoniques tenues une fois par semaine ou plus, mais aussi d'échanger des courriels sur sa liste de diffusion. En outre, l'équipe responsable de l'EPDP a tenu quatre réunions en personne : la première série de discussions en personne a eu lieu lors de la réunion publique ICANN65 à Marrakech, au Maroc, deux réunions en personne dédiées, la deuxième et la quatrième réunion, ont eu lieu au siège de l'ICANN à Los Angeles (LA) en septembre 2019 et janvier 2020, et la troisième discussion en personne s'est tenue lors de la réunion publique ICANN66 à Montréal, au Canada. Toutes les réunions de l'équipe responsable de l'EPDP sont documentées sur son espace de travail wiki, y compris sa liste de diffusion, les documents préliminaires, les documents d'information et les contributions provenant des organisations de soutien et des comités consultatifs de l'ICANN, y compris les groupes de parties prenantes et les unités constitutives de la GNSO.

L'équipe responsable de l'EPDP a également préparé un plan de travail qui a été révisé et mis à jour régulièrement. Afin de faciliter son travail, l'équipe responsable de l'EPDP a utilisé un modèle pour mettre sous forme de tableau toutes les données reçues en réponse à sa demande de déclarations aux groupes de parties prenantes et aux unités constitutives (consulter l'annexe D). Ce modèle a été utilisé pour enregistrer les commentaires demandés à d'autres organisations de soutien et comités consultatifs de l'ICANN qui se trouvent à l'annexe D.

L'équipe responsable de l'EPDP a tenu une séance communautaire pendant la réunion publique ICANN66 à Montréal, au cours de laquelle elle a présenté ses méthodes de travail et ses conclusions préliminaires à l'ensemble de la communauté de l'ICANN pour discussion et commentaires.

2.2 Carte heuristique, feuilles de travail et éléments de base

Afin d'assurer une compréhension commune des sujets à traiter dans le cadre de ses délibérations de l'étape 2, l'équipe responsable de l'EPDP a cartographié les sujets à l'aide des cartes heuristiques suivantes, qui ont permis le regroupement et la

consolidation des sujets à aborder (consulter la carte heuristique). Cela a constitué la base de l'élaboration ultérieure des feuilles de travail de priorité 1 et de priorité 2 (consulter les feuilles de travail) que l'équipe responsable de l'EPDP a utilisées pour saisir :

- La description du problème / les questions liées à la charte
- Le livrable attendu
- La lecture requise
- Les documents d'information qui doivent être fournis
- Les questions juridiques
- Les dépendances
- Le calendrier et approche proposés

Le président de l'équipe responsable de l'EPDP a également présenté un certain nombre de définitions de travail afin d'assurer une terminologie cohérente et une compréhension commune des termes utilisés lors des délibérations de l'équipe (consulter les définitions de travail).

Suite à l'examen d'un nombre de cas d'utilisation de la vie réelle, l'équipe responsable de l'EPDP a établi un ensemble d'éléments de base que le système normalisé d'accès et de divulgation (« SSAD ») pourrait comprendre, reconnaissant qu'une décision sur les rôles et les responsabilités des différentes parties concernées pourrait être influencée à la fois par les conseils juridiques et les avis du Conseil européen de la protection des données (« CEPD »).

2.3 Sujets de priorité 1 et de priorité 2

Afin d'organiser son travail, l'équipe responsable de l'EPDP a accordé de diviser son travail en deux ensembles de priorités : priorité 1 et priorité 2. La priorité 1 comprend le SSAD et toutes les questions directement liées. La priorité 2 comprend les questions suivantes :

- L'affichage d'information des sociétés affiliées versus les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire accrédités ;
- La distinction entre personnes morales et personnes physiques ;
- L'expurgation du champ « ville »
- La conservation de données
- L'objectif potentiel du bureau du directeur de la technologie de l'ICANN
- La possibilité pour les contacts uniques d'avoir une adresse e-mail anonymisée uniforme
- Le système de signalement de problèmes liés à l'exactitude du WHOIS

L'équipe responsable de l'EPDP a convenu que la priorité devrait être accordée à l'achèvement des délibérations pour les points de priorité 1. Il est toutefois convenu

que, dans la mesure du possible, l'équipe s'efforcera également de faire des progrès, parallèlement, sur les points de priorité 2.

En raison des dépendances externes et des contraintes temporelles, le présent rapport final n'aborde pas tous les points de priorité 2. Plus précisément, les éléments suivants ne sont pas traités :

La distinction entre personnes physiques et personnes morales : bien que la question ait été examinée à l'étape 2, cela n'a pas donné lieu à un accord sur les nouvelles recommandations de politique. L'étude demandée sur ce sujet a été reçue trop tard dans le processus pour être dûment prise en considération. Par conséquent, en vertu des recommandations de l'étape 1 de l'équipe responsable de l'EPDP les bureaux d'enregistrement et les opérateurs de registre sont autorisés à faire une distinction entre les enregistrements de personnes physiques et personnes morales sans, toutefois, être tenus de le faire. D'autres travaux sur cette question (y compris l'examen de la distinction établie par l'ICANN entre les personnes morales et les personnes physiques dans l'étude des services d'annuaire de données d'enregistrement de noms de domaine (RDDS)) sont en cours d'examen par le conseil de la GNSO.

Faisabilité d'une adresse e-mail anonymisée uniforme pour les contacts uniques : L'équipe responsable de l'EPDP a reçu des directives juridiques indiquant que la publication d'adresses e-mail anonymes uniformes entraîne la publication de données à caractère personnel ; ce qui montre qu'il peut ne pas être possible de publier une grande échelle d'adresses e-mail anonymes uniformes aux termes du RGPD. D'autres travaux sur cette question sont en cours d'examen par le conseil de la GNSO.

2.4 Comité juridique

Reconnaissant la complexité de nombreux problèmes que l'équipe responsable de l'EPDP a été chargée d'aborder à l'étape 2, l'équipe responsable de l'EPDP a demandé des ressources pour le conseiller juridique externe Bird & Bird. Afin d'aider à la préparation des questions juridiques préliminaires pour Bird & Bird, les dirigeants de l'EPDP ont décidé de constituer un comité juridique composé de membres de l'équipe responsable de l'EPDP ayant de l'expérience juridique.

Le Comité juridique de l'étape 2 a collaboré dans l'examen des questions proposées par les membres de l'équipe responsable de l'EPDP afin d'assurer que :

1. les questions soient de nature véritablement juridique, par opposition aux questions de politique ou de mise en œuvre des politiques ;
2. les questions aient été formulées de manière neutre, évitant à la fois des résultats présumés et le positionnement des unités constitutives ;

3. les questions soient à la fois posées de manière appropriée et en temps utile pour le travail de l'équipe responsable de l'EPDP ; et
4. le budget limité des avocats externes ait été utilisé de manière responsable.

Le Comité juridique a présenté toutes les questions convenues à l'équipe responsable de l'EPDP pour approbation finale avant d'envoyer des questions à Bird & Bird, à l'exception des questions sur l'automatisation de la prise de décisions.

À ce jour, l'équipe responsable de l'EPDP a accepté d'envoyer à Bird & Bird huit questions relatives au SSAD. Le texte intégral des questions et des résumés analytiques des avis juridiques reçus en réponse aux questions se trouvent à l'annexe F.

2.5 Questions de la charte

Pour répondre aux questions de la charte,[2] l'équipe responsable de l'EPDP a examiné (1) les commentaires fournis par chaque groupe dans le cadre des délibérations ; (2) les commentaires pertinents de l'étape 1 ; (3) les commentaires fournis par chaque groupe en réponse à la demande de contribution précoce concernant les questions spécifiques de la charte ; (4) la lecture requise identifiée pour chaque sujet dans les feuilles de travail ; (5) les commentaires fournis en réponse aux forums de commentaires publics et (6) les commentaires fournis par Bird & Bird, conseillers juridiques de l'équipe responsable de l'EPDP.

[2] L'annexe A traite plus en détail du lien entre chacun des sujets abordés dans les recommandations et les questions pertinentes de la charte.

3 Réponses de l'équipe responsable de l'EPDP aux questions de la charte et recommandations correspondantes

Après avoir examiné les commentaires publics sur le rapport initial et le supplément du rapport initial, l'équipe responsable de l'EPDP présente ces recommandations au conseil de la GNSO pour examen. Ce rapport final indique le niveau de consensus atteint au sein de l'équipe responsable de l'EPDP eu égard aux différentes recommandations. En bref :

- Onze (11) recommandations ont obtenu la désignation de consensus complet (1, 2, 3, 4, 11, 13, 15, 16, 17, 19 et 21)
- Trois (3) recommandations ont obtenu la désignation de consensus (7, 20 et 21)
- Six (6) recommandations ont fait l'objet d'un fort soutien mais avec des objections considérables (5, 8, 9, 10, 12 et 18)
- Deux (2) recommandations ont été signalées comme faisant l'objet de divergences (6 et 14)

Pour de plus amples détails sur ces désignations, veuillez consulter l'article 3.6 des Directives de la GNSO pour les groupes de travail.

Seulement en ce qui concerne les recommandations relatives au SSAD, l'équipe responsable de l'EPDP considère ces interdépendantes et, par conséquent, elles doivent être considérées comme un ensemble par le conseil de la GNSO et par la suite par le Conseil de l'ICANN.

Note : au cours de l'étape 1 du travail de l'équipe responsable de l'EPDP, cette dernière a été chargée d'examiner la Spécification temporaire. La Spécification temporaire a été établie en réponse au RGPD.[3] Par conséquent, le RGPD est la seule loi étant expressément mentionnée dans le présent rapport. L'équipe responsable de l'EPDP a délibéré sur la question de savoir si ce rapport final pouvait être rédigé d'une manière qui soit indépendante de toute loi spécifique, mais elle a déterminé que le rapport bénéficierait de références explicites pour faciliter la mise en œuvre des recommandations de l'équipe. Le RGPD est une loi régionale couvrant plusieurs juridictions et, compte tenu des critères stricts qu'il contient, le respect de cette loi a une forte probabilité d'être conforme à d'autres lois nationales ou régionales applicables en matière de protection des données. L'équipe responsable de l'EPDP

[3] « La présente Spécification temporaire relative aux données d'enregistrement des gTLD (la Spécification temporaire) pose des exigences temporaires visant à permettre à l'ICANN et aux opérateurs de registre et bureaux d'enregistrement des gTLD de respecter les exigences contractuelles de l'ICANN et les politiques définies par la communauté à la lumière du RGPD ».

souscrit pleinement à l'intention de l'ICANN d'être globalement inclusive, et rien dans ce rapport n'annulera le principe de base selon lequel les parties contractantes peuvent et doivent se conformer aux lois et réglementations locales applicables.

3.1 Système normalisé d'accès et de divulgation aux données d'enregistrement non publiques (SSAD)

L'annexe A présente de plus amples détails sur l'approche et les documents que l'équipe responsable de l'EPDP a examinés afin de répondre aux questions de la charte et d'élaborer les recommandations suivantes.

Dans le cadre de ses délibérations, l'équipe responsable de l'EPDP a considéré un modèle centralisé, où les requêtes et les décisions de divulgation seraient gérées par l'organisation ICANN ou un sous-traitant délégué, et un modèle décentralisé, où les requêtes et les décisions de divulgation seraient gérées par les parties contractantes. L'équipe n'a pas réussi à se mettre d'accord sur l'une ou l'autre option, si bien qu'elle a proposé un modèle hybride où les requêtes seraient centralisées et les décisions de divulgation seraient (en principe, lors de la mise en œuvre initiale) prises par les parties contractantes. Le modèle hybride SSAD est basé sur les principes de haut niveau suivants :

- La réception, l'authentification et la transmission des requêtes SSAD à la partie contractante doivent être entièrement automatisées dans la mesure où elles soient techniquement et commercialement réalisables et permises par la loi. Les décisions de divulgation seront généralement prises (lors de la mise en œuvre initiale) par la partie contractante et ne devraient être automatisées qu'aux cas où cela serait techniquement et commercialement faisable et permis par la loi. Dans les domaines où l'automatisation ne répond pas à ces critères, la normalisation du processus décisionnel en matière de divulgation est l'objectif de base. L'expérience acquise au fil du temps avec les requêtes de divulgation et les réponses du SSAD doit éclairer davantage la rationalisation et la normalisation des réponses.
- En reconnaissance de la nécessité d'ajustements basés sur l'expérience dans la fonction du SSAD, il devrait y avoir un comité permanent de la GNSO qui surveille la mise en œuvre du SSAD et recommande les améliorations qui pourraient être apportées. Les améliorations recommandées dans le cadre de ce processus ne doivent pas enfreindre les politiques établies par l'EPDP, les lois sur la protection des données, les statuts constitutifs de l'ICANN ou les procédures et directives de la GNSO.
- Les conventions de service (SLA) doivent être mises en place et être applicables, mais elles peuvent devoir changer au fil du temps pour reconnaître qu'il y aura une courbe d'apprentissage.

- Les réponses aux requêtes de divulgation, indépendamment du fait que la révision soit effectuée manuellement ou qu'une réponse automatique soit déclenchée, sont renvoyées directement au requérant par la partie contractante concernée. Toutefois, des mécanismes de connexion appropriés doivent être mis en place pour permettre au SSAD de confirmer que les SLA soient respectés et que les réponses soient traitées conformément à la politique (par exemple, la passerelle centrale DOIT être notifiée lorsque les demandes de divulgation sont rejetées ou accordées).

Les bénéfices de ce modèle sont :

Un emplacement unique pour soumettre les demandes

- La réduction du temps et des efforts consacrés par les requérants pour faire le suivi des points de contact individuels ou des procédures individuelles
- L'assurance que les requêtes sont acheminées directement à la partie responsable de chaque entité divulgatrice, éliminant ainsi l'incertitude quant au fait que les requêtes ne soient pas reçues ou qu'elles soient transmises à une personne non qualifiée pour les traiter
- La capacité d'offrir des opportunités de communication claires pour socialiser l'emplacement et la méthode de demande de données d'enregistrement non publiques
- Les requêtes et les réponses peuvent faire l'objet d'un suivi pour voir si elles sont conformes aux SLA

Formulaires de requête normalisés

- Réduction du nombre de requêtes de divulgation refusées à cause d'informations insuffisantes
- Augmentation de l'efficacité avec laquelle les entités divulgatrices peuvent examiner les requêtes
- Réduction de l'incertitude pour les requérants qui disposent désormais d'un ensemble de données normalisées/uniformes à fournir lors de la soumission des requêtes de divulgation.
- Réduction du besoin d'un ensemble individuel d'informations requises par les parties divulgatrices

Processus d'authentification intégré

- Accélère le processus de révision pour les entités divulgatrices car celles-ci n'auront pas besoin de vérifier à nouveau le requérant
- L'assurance externe que les requérants ont été vérifiés peut augmenter le probabilité et/ou la rapidité de la divulgation

Processus normalisé de révision et de réponse

- Permet la création d'un format de réponse commun

- Permet la création de règles, de lignes directrices et de meilleures pratiques que les parties divulgatrices peuvent suivre lors de la révision et de la réponse aux requêtes
- Permet l'adoption d'un système commun de révision des réponses
- Permet l'automatisation de certaines requêtes à définir par les requérants
- Facilite la prise de décisions automatisée en matière de divulgation dans certains scénarios
- La journalisation des requêtes et des réponses permet également à l'organisation ICANN d'auditer les actions des entités divulgatrices, d'identifier les cas de non-conformité systémique et de prendre les mesures d'application appropriées

Principaux rôles et responsabilités du SSAD :

- Gestionnaire de la passerelle centrale – rôle exécuté ou supervisé par l'organisation ICANN. Responsable de la gestion de la prise en charge et de l'acheminement des requêtes SSAD qui nécessitent une révision manuelle des parties contractantes responsables. Responsable de la gestion et de l'acheminement de l'automatisation des requêtes confirmées afin que les parties contractantes publient les données, conformément aux critères établis et convenus dans ces recommandations de politique générale ou sur la base de la recommandation du comité permanent de la GNSO pour la révision de la mise en œuvre des recommandations de politique concernant le SSAD. Responsable de la collecte des données sur les requêtes, les réponses et les décisions de divulgation ayant été prises.
- Autorité d'accréditation – rôle exécuté ou supervisé par l'organisation ICANN. Une entité de gestion désignée pour avoir l'autorité formelle d'« accréditer » les utilisateurs du SSAD, c'est-à-dire de confirmer et de vérifier l'identité de l'utilisateur (représenté par des données d'identification) et les assertions (ou réclamations) associées aux données d'identification (représentés par des assertions signées).
- Fournisseur d'identité - responsable de 1) vérifier l'identité d'un demandeur et gérer les données d'identification associées au demandeur, 2) vérifier et gérer les assertions signées associées aux données d'identification. Aux fins du SSAD, le fournisseur d'identité peut être l'autorité d'accréditation elle-même ou bien cette dernière peut compter sur aucun ou plusieurs tiers pour exécuter les services du fournisseur d'identité.
- Parties contractantes – responsables de répondre aux demandes de divulgation qui ne satisfont pas aux critères pour une réponse automatisée.[4]

[4] Par défaut, le gestionnaire de la passerelle centrale enverra les requêtes de divulgation aux bureaux d'enregistrement, ce qui n'empêchera pas le gestionnaire de la passerelle centrale d'envoyer des requêtes de divulgation aux opérateurs de registre dans certaines circonstances (pour de plus amples détails, consulter la Recommandation 5).

- Comité permanent de la GNSO pour la révision de la mise en œuvre des recommandations de politique concernant le SSAD – Représentant du comité de la communauté de l'ICANN responsable de l'évaluation des questions opérationnelles du SSAD émergeant suite à l'adoption des politiques de consensus de l'ICANN et/ou de leur mise en œuvre. Le Comité permanent de la GNSO a pour but d'examiner les données produites à la suite des opérations du SSAD et de fournir au conseil de la GNSO des recommandations sur la meilleure façon d'apporter des changements opérationnels au SSAD, qui sont strictement des mesures de mise en œuvre, en plus des recommandations fondées sur l'examen de l'impact des politiques de consensus existantes sur les opérations du SSAD.

On s'attend à ce que les différents rôles et responsabilités soient décrits en détail et confirmés dans les accords applicables.

Vous trouverez ci-dessous une répartition détaillée des hypothèses sous-jacentes et des recommandations de politique que l'équipe responsable de l'EPDP a présentées pour connaître l'avis de la communauté.

3.2 Contribution du Conseil d'administration de l'ICANN et de l'organisation ICANN

Afin de contribuer à éclairer ses délibérations, l'équipe responsable de l'EPDP a contacté le Conseil d'administration de l'ICANN et l'organisation ICANN pour « comprendre la position du Conseil sur la portée de la responsabilité opérationnelle et le niveau d'engagement (lié à la prise de décisions sur la divulgation des données d'enregistrement non publiques) qu'ils sont prêts à accepter au nom de l'organisation ICANN, ainsi que toutes les conditions préalables qui pourraient avoir besoin d'être remplies pour ce faire ».

Le 19 novembre, l'organisation ICANN a donné sa réponse, notant en partie que « l'organisation ICANN a proposé l'exploitation d'une passerelle pour faire passer les données autorisées. Tel que mentionné ci-dessus, l'exploitant de la passerelle ne prend pas la décision d'autoriser la divulgation. Dans le modèle proposé, le fournisseur de l'autorisation déciderait si les critères de divulgation sont satisfaits ou non. Si une demande était autorisée et authentifiée, l'opérateur de la passerelle demanderait les données à la partie contractante et communiquerait l'ensemble des données pertinentes au requérant.[5]

Le 20 novembre 2019, le Conseil d'administration de l'ICANN a donné sa réponse en signalant en partie que « le Conseil d'administration a toujours préconisé le

[5] Veuillez noter que le modèle décrit ici n'est pas le même que le modèle SSAD a présenté dans le présent rapport par l'équipe responsable de l'EPDP.

développement d'un modèle d'accès aux données d'enregistrement de gTLD non publiques. Si le travail de l'étape 2 de l'équipe responsable de l'EPDP aboutissait à une recommandation consensuelle selon laquelle l'organisation ICANN assume la responsabilité d'une ou de plusieurs fonctions opérationnelles au sein d'un SSAD, le Conseil d'administration adopterait cette recommandation à moins qu'il n'ait déterminé, par un vote de plus des deux tiers, qu'une telle politique ne serait pas dans l'intérêt de l'ICANN ou de sa communauté. Compte tenu de la défense par le Conseil d'administration de l'élaboration d'un modèle d'accès et de soutien au dialogue de l'organisation ICANN avec le CEPD sur une proposition d'UAM, il est probable que le Conseil adopte une recommandation de l'EPDP à cet effet.

L'équipe responsable de l'EPDP a posé un certain nombre de questions de clarification supplémentaires à l'organisation ICANN que vous trouverez, avec les réponses, ici : https://community.icann.org/x/5BdIBg. Cette contribution comprenait également l'estimation des coûts de l'organisation ICANN pour un système proposé d'accès et de divulgation normalisé.

L'équipe responsable de l'EPDP a examiné cette contribution, les commentaires reçus de l'APD belge et les commentaires reçus pendant la période de consultation publique afin de déterminer de façon définitive la répartition des rôles et responsabilités dans le SSAD.

3.3 Hypothèses sous-jacentes du SSAD

L'équipe responsable de l'EPDP a utilisé les hypothèses sous-jacentes décrites ci-dessous pour élaborer ses recommandations de politique. Ces hypothèses sous-jacentes ne créent pas nécessairement de nouvelles exigences pour les parties contractantes ; les hypothèses sont plutôt conçues pour aider les lecteurs du présent rapport final et les responsables de la mise en œuvre de la politique finale à comprendre l'intention et les hypothèses sous-jacentes de l'équipe responsable de l'EPDP pour proposer le modèle du SSAD et les recommandations connexes.

- L'objectif du SSAD est de fournir un mécanisme prévisible, transparent, efficace et fiable pour l'accès et la divulgation des données d'enregistrement non-publiques.
- Le SSAD doit être conforme au RGPD.
- Le SSAD doit avoir la capacité de respecter ces principes de politique et ces recommandations.
- Compte tenu des décisions prises par l'équipe responsable de l'EPDP concernant le modèle SSAD, l'hypothèse de travail est que l'ICANN et les parties contractantes seront des responsables conjoints du traitement. Cette désignation est fondée sur une analyse factuelle de la politique telle qu'elle est proposée.

3.4 Conventions utilisées dans ce document

Les termes clés « DOIT », « NE DOIT PAS », « REQUIS », « DEVRA », « NE DEVRA PAS », « DEVRAIT », « NE DEVRAIT PAS », « RECOMMANDÉ », « NON RECOMMANDÉ », « POURRAIT » et « FACULTATIF » utilisés dans le présent document seront interprétés tel que décrit dans le BCP 148, le RFC2119, et le RFC8174.

Remarque : notant le choix du modèle par l'équipe responsable de l'EPDP, et dans l'attente des conseils juridiques spécifiques concernant la responsabilité des parties et l'identification du contrôle des données, comme il s'applique au modèle proposé, l'équipe responsable de l'EPDP signale que, dans le cadre des recommandations, certaines déclarations peuvent nécessiter un peaufinement des degrés d'applicabilité allant d'obligatoire à permissif et vice versa. (Par exemple, « devrait » au lieu de « devra », « POURRAIT » au lieu de « DOIT », etc.).

Lorsque l'on fait référence aux orientations de la mise en œuvre, l'équipe responsable de l'EPDP considère ce contexte supplémentaire et/ou les précisions sur les renseignements pour aider à éclairer la mise en œuvre des recommandations de politique, mais l'équipe responsable de l'EPDP note que l'orientation de la mise en œuvre n'a ni le même poids ni le même statut que le texte d'une recommandation pour créer une politique.

3.5 Recommandations de l'équipe responsable de l'EPDP au SSAD

3.5.1. Définitions

- **Accréditation** : action administrative par laquelle l'autorité d'accréditation déclare qu'un utilisateur est autorisé à utiliser le SSAD dans une configuration de sécurité particulière avec un ensemble prescrit de garanties.
- **Autorité d'accréditation :** entité de gestion désignée pour avoir l'autorité formelle d'« accréditer » les utilisateurs du SSAD, c'est-à-dire de confirmer et de vérifier l'identité de l'utilisateur (représenté par des données d'identification) et les assertions (ou réclamations) associées aux données d'identification (représentées par des assertions signées).
- **Auditeur de l'autorité d'accréditation** : entité responsable de l'exécution des exigences de vérification de l'autorité d'accréditation, tel qu'indiqué dans la recommandation 16 (Audits). L'entité pourrait être un organisme indépendant ou, si l'organisation ICANN délimitait le rôle d'autorité d'accréditation à un tiers, l'organisation ICANN POURRAIT devenir l'auditeur de l'autorité d'accréditation.
- **Authentification :** processus ou action de validation des informations d'identification et des assertions signées d'un requérant.

- **Autorisation :** processus permettant d'approuver ou de refuser la divulgation de données d'enregistrement non publiques.
- **Gestionnaire de la passerelle centrale (CGM) :** rôle exécuté ou supervisé par l'organisation ICANN. Responsable de la gestion de la prise en charge et de l'acheminement des requêtes SSAD qui nécessitent une révision manuelle des parties contractantes responsables. Responsable de la gestion et de l'acheminement de l'automatisation des requêtes confirmées afin que les parties contractantes publient les données, conformément aux critères établis et convenus dans ces recommandations de politique générale ou sur la base de la recommandation du comité permanent de la GNSO pour la révision de la mise en œuvre des recommandations de politique concernant le SSAD. Responsable de la collecte des données sur les requêtes, les réponses et les décisions de divulgation ayant été prises.
- **Désaccréditation de l'autorité d'accréditation :** action administrative par laquelle l'organisation ICANN révoque le contrat avec l'autorité d'accréditation, si cette fonction était externalisée à un tiers, après quoi elle ne serait plus autorisée à fonctionner comme autorité d'accréditation.
- **Entité gouvernementale admissible** : une entité gouvernementale (y compris les administrations locales et les organisations internationales gouvernementales) qui a pour but d'accéder aux données d'enregistrement non publiques pour l'exercice d'une fonction de politique publique dans le cadre de son mandat.
- **Données d'identification :** objet de données qui est une représentation portable de l'association entre un identificateur et des informations authentifiées et qui peut être présenté pour la validation d'une identité réclamée par une entité qui tente d'accéder à un système. Exemple : nom d'utilisateur/mot de passe, données d'identification OpenID, certificat de clé publique X.509.
- **Fournisseur d'identité :** responsable de 1) vérifier l'identité d'un requérant et gérer les données d'identification associées au requérant et 2) vérifier et gérer les assertions signées associées aux données d'identification. Aux fins du SSAD, le fournisseur d'identité peut être l'autorité d'accréditation elle-même ou bien cette dernière peut compter sur aucun ou plusieurs tiers pour exécuter les services du fournisseur d'identité.
- **Requérant :** utilisateur accrédité cherchant à accéder aux données d'enregistrement de nom de domaine par le biais du SSAD.
- **Révocation des données d'identification de l'utilisateur :** événement qui se produit lorsqu'un fournisseur d'identité déclare que des données d'identification valides au préalable sont devenues non valides.
- **Assertion signée** : objet de données qui est une représentation portable de l'association entre les données d'identification et une ou plusieurs assertions d'accès et qui peut être présenté pour la validation de ces assertions par une entité qui tente ce type d'accès. Exemple : [Données d'identification OAuth], certificat d'attribut X.509. Les assertions signées peuvent être spécifiques à

l'utilisateur (par exemple, pour indiquer une affiliation professionnelle ou une affirmation de processus de traitement licite de données) ou spécifiques à une requête (par exemple, pour indiquer la base juridique de la requête de divulgation).

- **Système normalisé d'accès et de divulgation aux données d'enregistrement pour les données d'enregistrement de gTLD non publiques** (SSAD) : le SSAD est la suite globale des parties et des mécanismes qui constituent le système de requête, de validation et de divulgation.
- **Valider/validation :** tester, prouver ou établir la validité ou l'exactitude d'une construction. (Exemple : le divulgateur validera les données d'identification et les assertions signées dans le cadre de son processus d'autorisation).
- **Vérifier :** tester ou prouver la vérité ou l'exactitude d'un fait ou d'une valeur. (Exemple : les fournisseurs d'identité vérifient l'identité du requérant avant d'émettre les données d'identification).
- **Vérification :** processus d'examen de l'information pour revendiquer un fait ou une valeur.

3.5.2. Recommandations

Recommendation #1. Accréditation[6]

1.1. L'équipe responsable de l'EPDP recommande la création ou la sélection d'une autorité d'accréditation.

1.2. L'équipe responsable de l'EPDP recommande que l'autorité d'accréditation établisse une politique d'accréditation des utilisateurs du SSAD conformément aux recommandations ci-dessous.

1.3. Les recommandations suivantes DOIVENT être incluses dans la politique d'accréditation :

1.3.1. Le SSAD DOIT accepter uniquement les requêtes d'accès ou de divulgation émanant de personnes physiques ou morales accréditées. Toutefois, les exigences d'accréditation DOIVENT s'adapter à tout utilisateur prévu du système, y compris une personne ou une organisation qui envoie une seule requête. Les exigences d'accréditation pour les utilisateurs réguliers du système et pour un utilisateur unique du système POURRAIENT différer.

1.3.2. Les personnes morales et/ou les personnes physiques sont admissibles à l'accréditation. Une personne qui accède au SSAD à l'aide des données d'identification d'une entité accréditée (par exemple des personnes

[6] Il convient de noter que l'accréditation ne fait pas référence à l'accréditation/la certification, comme cela est expliqué dans les articles 42/43 du RGPD.

morales) garantit que la personne agit au titre de l'autorité de l'entité accréditée.

1.3.3. La politique d'accréditation définit une autorité d'accréditation unique, gérée par l'organisation ICANN, qui est responsable de la vérification, de l'émission et de la gestion continue des données d'identification et des assertions signées. L'autorité d'accréditation DOIT élaborer une politique en matière de vie privée. L'autorité d'accréditation POURRAIT travailler avec des fournisseurs d'identité externes ou tiers qui pourraient servir de centres d'échange pour vérifier les informations d'identité et d'autorisation associées aux personnes requérant l'accréditation. La responsabilité du traitement des données à caractère personnel, quelle que soit la partie qui effectue ce traitement, est du ressort de l'autorité d'accréditation. Si l'organisation ICANN choisit d'externaliser la fonction de l'autorité d'accréditation ou des parties de celle-ci, l'organisation ICANN restera responsable de la supervision des parties auxquelles la fonction ou les parties de la fonction sont externalisées. La supervision DOIT inclure la surveillance et la gestion des abus potentiels par la ou les parties auxquelles la fonction de parties de celles-ci a été externalisée.

1.3.4. La décision d'autoriser la divulgation des données d'enregistrement, fondée sur la validation des données d'identification, des assertions signées et des données requises dans la recommandation concernant les critères et le contenu des requêtes (Recommandation 3), appartiendra au bureau d'enregistrement, à l'opérateur de registre ou au gestionnaire de la passerelle centrale, selon le cas.

1.4. Exigences de l'autorité d'accréditation

1.4.1. Vérifier l'identité du requérant : L'autorité d'accréditation DOIT vérifier l'identité du requérant, ce qui entraîne la création des données d'identification.

1.4.2. Gestion des assertions signées : L'autorité d'accréditation POURRAIT vérifier et gérer un ensemble d'assertions/réclamations dynamiques associées et liées à l'identité du requérant. Cette vérification, qui peut être effectuée par un fournisseur d'identité, aboutit à une assertion signée. Les assertions signées[7] transmettent des informations telles que :

[7] Pour plus de clarté, les assertions signées sont dynamiques et peuvent changer en fonction de la requête (finalité, base juridique, type, urgence, etc.) par rapport à une donnée d'identification, qui est statique et ne change généralement pas. Les assertions signées ne sont utilisées que pour associer/lier des attributs à une identité. Ces attributs sont dynamiques par requête, mais peuvent être contrôlés et gérés dès le début dans le cadre du processus d'accréditation, selon les besoins. L'autorité d'accréditation peut établir diverses assertions pour des données d'identification spécifiques ou les créer de façon dynamique en fonction des requêtes. Les détails à propos de la façon dont cela est déterminé restent à définir lors de l'étape de mise en œuvre. L'autorité d'accréditation peut stocker plusieurs assertions signées par donnée d'identification, mais le demandeur doit invoquer les assertions pertinentes par demande.

- L'assertion quant au(x) finalité(s) de la demande
- L'assertion quant à la base juridique de la demande
- L'assertion selon laquelle l'utilisateur identifié par les données d'identification est affilié à l'organisation concernée
- L'assertion concernant le respect des lois (par exemple, stockage, protection et conservation/élimination des données)
- L'assertion concernant l'accord pour utiliser des données divulguées à des finalités légitimes et légales énoncées
- L'assertion concernant le respect des garanties et/ou des conditions de service, sujette à la révocation au cas où elles seraient fautives
- Les assertions concernant la prévention des abus, les exigences en matière d'audit, les processus de règlement de litiges et de traitement des plaintes, etc.
- Les assertions spécifiques au requérant – propriété/enregistrement de marque, par exemple
- Les déclarations de procuration, le cas échéant.

1.4.3. DOIT valider les données d'identification et les assertions signées, en plus des informations contenues dans la requête, et faciliter la décision d'accepter ou de rejeter l'autorisation d'une requête au SSAD. Pour dissiper tout doute, la seule présence de ces références d'identité NE DOIT PAS entraîner ou exiger une autorisation d'accès/divulgation automatique. Toutefois, la capacité d'automatiser la prise de décisions en matière d'autorisation d'accès et de divulgation est possible dans certaines circonstances au cas où celle-ci serait légale.

1.4.4. L'autorité d'accréditation DOIT définir un « code de conduite » de base[8] qui établisse un ensemble de règles qui contribuent à l'application correcte des lois sur la protection des données, telles que le RGPD, notamment :

- Un exposé des motifs clair et concis.
- Une portée définie qui détermine les opérations de traitement couvertes (l'accent du SSAD devrait être mis sur l'opération de divulgation).
- Mécanisme qui permet de surveiller le respect des dispositions.
- Identification d'un auditeur de l'autorité d'accréditation (dit organe de surveillance) et définition du ou des mécanisme(s) permettant à cet organe de s'acquitter de ses fonctions.
- Description quant à la mesure dans laquelle une « consultation » avec les parties prenantes a été effectuée.

1.4.5. L'autorité d'accréditation DOIT élaborer une politique en matière de vie privée pour le traitement des données personnelles qu'elle entreprend

[8] Afin d'éviter toute confusion, le code de conduite mentionné ici n'a pas pour objet de se référer au Code de conduite tel que décrit dans le RGPD. Le code de conduite mentionné ici fait référence à un ensemble de règles et de normes devant être suivies par l'autorité d'accréditation.

ainsi que des conditions de service pour ses utilisateurs accrédités (comme indiqué dans la Recommandation 11).

1.4.6. Élaborer une procédure de demande de base : L'autorité d'accréditation DOIT élaborer une procédure de demande de base uniforme et des exigences connexes pour tous les fournisseurs d'identité (le cas échéant) et pour tous les demandeurs sollicitant l'accréditation, y compris :
   i. Le calendrier d'accréditation
   ii. La définition des critères d'admissibilité pour les utilisateurs accrédités
   iii. La validation de l'identité, les procédures
   iv. Les politiques de gestion des données d'identification : durée de vie/expiration, fréquence de renouvellement, propriétés de sécurité (mot de passe ou stratégies de clé/force), etc.
   v. Procédures de révocation des informations d'identité : circonstances de la révocation, mécanisme(s) de révocation, etc. (consulter également la section « Révocation et abus des utilisateurs accrédités » ci-dessous)
   vi. Gestion des assertions signées : durée de vie/expiration, fréquence de renouvellement, etc.
   vii. REMARQUE : des exigences au-delà de la ligne de base indiquée ci-dessus peuvent s'avérer nécessaires pour certaines classes de requérants.

1.4.7. Définition du processus de règlement de litiges et de plaintes : l'autorité d'accréditation DOIT définir un processus de règlement de litiges et de plaintes pour contester les mesures prises par l'autorité d'accréditation. Le processus défini DOIT inclure les contrôles et contrepoids de la diligence raisonnable.

1.4.8. Audits : L'autorité d'accréditation DOIT être vérifiée régulièrement par un auditeur. Si l'autorité d'accréditation est jugée non conforme à la politique et aux exigences d'accréditation, elle aura la possibilité de remédier à la violation, mais en cas de défaillance répétée, une nouvelle autorité d'accréditation devra être identifiée ou créée. En outre, les entités accréditées DOIVENT être vérifiées régulièrement pour s'assurer de leur conformité à la politique et aux exigences d'accréditation (remarque : des informations détaillées sur les exigences d'audit pour l'autorité d'accréditation et les fournisseurs d'identité qu'elle peut utiliser sont disponibles dans la Recommandation d'audit n° 16).

1.4.9. Groupes d'utilisateurs : L'autorité d'accréditation POURRAIT développer des groupes/catégories d'utilisateurs pour faciliter le processus d'accréditation, car tous les demandeurs devront être accrédités, et l'accréditation inclura la vérification de l'identité.

1.4.10. Rapports : L'autorité d'accréditation DOIT rendre compte publiquement et régulièrement du nombre de demandes d'accréditation reçues, des demandes d'accréditation approuvées/renouvelées, des accréditations refusées, des accréditations révoquées, des plaintes reçues et des

informations sur les fournisseurs d'identité avec qui elle travaille. Consulter aussi la Recommandation 17 et les rapports

1.4.11. Renouvellement : L'autorité d'accréditation DOIT établir un calendrier et des exigences pour le renouvellement de l'accréditation.

1.4.12. Confirmation des données du titulaire du nom de domaine : L'autorité d'accréditation DOIT envoyer des rappels périodiques (par exemple, tous les ans) aux utilisateurs accrédités pour confirmer les données de l'utilisateur et rappeler aux utilisateurs accrédités de tenir à jour les informations requises pour l'accréditation. Toute modification apportée à ces informations peut entraîner la nécessité d'une nouvelle accréditation.

1.5. Révocation d'un utilisateur accrédité

1.5.1. La révocation, dans le contexte du SSAD, signifie que l'autorité d'accréditation peut révoquer le statut d'utilisateur accrédité du SSAD.[9] Une liste non exhaustive d'exemples où la révocation peut s'appliquer comprend : 1) la violation par l'utilisateur accrédité de toute garantie ou condition de service applicable ; 2) un changement d'affiliation de l'utilisateur accrédité ; 3) une violation des exigences de conservation/destruction des données ou 4) lorsque les conditions préalables à l'accréditation n'existent plus.

1.5.2. L'autorité d'accréditation DOIT mettre à disposition un mécanisme d'appel pour permettre à un utilisateur accrédité de contester la décision de révocation du statut de l'utilisateur accrédité dans un délai déterminé par l'autorité d'accréditation. Toutefois, pour la durée de l'appel, le statut de l'utilisateur accrédité restera suspendu. Les résultats d'un appel DOIVENT être informés de manière transparente**.**

1.5.3. Un mécanisme pour signaler la violation par un utilisateur accrédité de toute garantie ou de toute condition de service DOIT être fourni par le SSAD.[10] Les rapports DOIVENT être transmis à l'autorité d'accréditation pour traitement. L'autorité d'accréditation POURRAIT également obtenir des renseignements d'autres parties pour déterminer que des abus ont eu lieu.

1.5.4. La politique de révocation pour les personnes/entités DEVRAIT inclure des sanctions progressives ; les sanctions seront plus détaillées pendant la mise en œuvre, en tenant compte de la manière dont les sanctions progressives sont appliquées dans d'autres domaines de l'ICANN. Autrement dit, toutes les violations du système n'entraînent pas la révocation ; toutefois, la révocation POURRAIT se produire si l'autorité

[9] Pour plus de clarté, une entité juridique ne serait pas automatiquement désaccréditée pour l'action unique d'un utilisateur individuel dont l'accréditation est liée à l'accréditation de l'entité juridique, mais l'entité peut être tenue responsable des actions de l'utilisateur individuel dont l'accréditation est liée à celle de l'entité juridique.

[10] À noter que l'abus du SSAD par un utilisateur accrédité est traité dans la Recommandation 13.

d'accréditation déterminait que la personne ou l'entité accréditée a enfreint de manière importante les conditions de son accréditation et n'a pas réussi à résoudre le problème en raison de : i) une plainte reçue, vérifiée par un tiers ; ii) les résultats d'un audit ou d'une enquête par l'autorité d'accréditation ou l'auditeur ; iii) tout mauvais usage ou abus des privilèges accordés ; iv) les violations répétées de la politique d'accréditation ; v) les résultats d'un audit ou d'une enquête par une APD.

1.5.5. En cas de comportement abusif par une personne ou une entité, les données d'identification de la personne ou de l'entité POURRAIENT être suspendues ou révoquées dans le cadre d'une sanction progressive.

1.5.6. La révocation DOIT empêcher la ré-accréditation à l'avenir en l'absence de circonstances particulières présentées à la satisfaction de l'autorité d'accréditation.

1.5.7. Afin d'éviter toute confusion, la désaccréditation n'empêche pas les individus ou les entités de présenter des demandes futures selon la méthode d'accès prévue dans la Recommandation 18 (demandes raisonnables de divulgation légale) du rapport de l'étape 1 de l'EPDP.

1.6. Annulation de l'autorisation des fournisseurs d'identité

1.6.1. Annulation de l'autorisation des fournisseurs d'identité : Les procédures de validation des fournisseurs d'identité DEVRAIENT inclure des pénalités progressives. Autrement dit, toutes les violations du système n'entraîneront pas l'annulation de l'autorisation ; toutefois, ladite annulation pourrait se produire si l'autorité d'accréditation déterminait que la personne ou l'entité accréditée n'a vraiment pas respecté les conditions de son accréditation et n'a pas réussi à résoudre le problème en raison de : i) une plainte reçue vérifiée par un tiers ; ii) les résultats d'un audit ou d'une enquête par l'autorité d'accréditation ou l'auditeur ; iii) tout mauvais usage ou abus des privilèges accordés ; iv) les violations répétées à la politique d'accréditation. En fonction de la nature et des circonstances ayant conduit à l'annulation de l'autorisation d'un fournisseur d'identité, certaines ou toutes ses données d'identification valides peuvent être révoquées ou transférées à un autre fournisseur d'identité.

1.6.2. L'autorité d'accréditation DOIT mettre à disposition un mécanisme d'appel pour permettre à un fournisseur d'identité de contester la décision d'annuler l'autorisation du fournisseur d'identité. Toutefois, pour la durée de l'appel, le statut du fournisseur d'identité restera suspendu. Les résultats d'un appel DOIVENT être signalés de manière transparente.

1.7. Considérations supplémentaires pour les entités ou les personnes accréditées :

1.7.1. Elles DOIVENT accepter :

1.7.1.1. d'utiliser seulement les données aux fins légitimes et légales énoncées ;

1.7.1.2. les conditions de service, dans lesquelles sont décrites les utilisations licites des données ;

1.7.1.3. de prévenir l'utilisation malveillante des données reçues ;

1.7.1.4. de coopérer avec toute demande d'audit ou d'information en tant que composante d'un audit ;

1.7.1.5. d'être soumis à l'annulation de l'accréditation au cas où on trouverait une utilisation malveillante des exigences ou de la politique en matière d'accréditation ;

1.7.1.6. de stocker, protéger et éliminer les données d'enregistrement de gTLD conformément à la loi applicable ;

1.7.2. Conserver uniquement les données d'enregistrement gTLD aussi longtemps que nécessaire pour atteindre l'objectif indiqué dans la demande de divulgation.

1.7.3. Le nombre de demandes SSAD qui peuvent être soumises pendant une période donnée NE DOIT PAS être limité, sauf si l'entité accréditée représente une menace démontrable au SSAD, ou si elles peuvent être autrement restreintes en vertu des présentes recommandations (comme par exemple en vertu des Recommandations 1.5(d) et 13(b)). Il est entendu que d'éventuelles limitations de la capacité de réponse et de la vitesse du SSAD peuvent être appliquées.

1.7.4. DOIVENT tenir à jour les informations requises pour l'accréditation et la vérification et informer rapidement l'autorité d'accréditation en cas de modification de ces informations. Tout changement POURRAIT entraîner de nouvelles accréditations ou la vérification de certaines informations fournies.

Orientations relatives à la mise en œuvre

1.8. En ce qui concerne l'accréditation, l'équipe responsable de l'EPDP fournit les orientations relatives à la mise en œuvre suivantes, sachant que des détails supplémentaires seront élaborés au cours de l'étape de mise en œuvre :

1.8.1. Des organisations reconnues, applicables et bien établies pourraient soutenir l'autorité d'accréditation en tant que fournisseur d'identité. Une vérification appropriée, telle que décrite au paragraphe 1.3(f) ci-dessus, DOIT avoir lieu si des organisations de bonne réputation et bien établies devaient collaborer avec l'autorité d'accréditation.

1.8.2. Voici quelques exemples d'informations supplémentaires que l'autorité d'accréditation ou le fournisseur d'identité POURRAIT exiger d'un candidat pour l'accréditation :
- un numéro d'enregistrement d'entreprise et le nom de l'autorité qui a émis ce numéro (si l'entité qui demande l'accréditation est une personne morale) ;
- des informations justifiant la propriété de la marque.[11]

1.9. Audit / journalisation par l'autorité d'accréditation et les fournisseurs d'identité

1.9.1. L'activité d'accréditation/vérification (telle que la demande d'accréditation, l'information selon laquelle a été prise la décision d'accréditer ou de vérifier l'identité) sera enregistrée par l'autorité d'accréditation et les fournisseurs d'identité.

1.9.2. Les données consignées NE DEVRONT être divulguées ou mises à disposition pour examen QUE par l'autorité d'accréditation ou le fournisseur d'identité, lorsque la divulgation sera jugée nécessaire pour a) remplir ou satisfaire à une obligation légale applicable de l'autorité d'accréditation ou du fournisseur d'identité ; b) effectuer un audit en vertu de la présente politique ; ou c) soutenir le fonctionnement raisonnable du SSAD et la politique d'accréditation.

Pour de plus amples informations, reportez-vous également à la section concernant les recommandations d'audit et les pratiques de journalisation.

1.10. Vérification. L'organisation ICANN devrait utiliser son expérience dans d'autres domaines où la vérification est impliquée, comme l'accréditation des bureaux d'enregistrement, pour présenter une proposition de vérification de l'identité du demandeur pendant l'étape de mise en œuvre.

1.11. Périodes de ré-accréditation. Comme meilleure pratique, la période de ré-accréditation et les exigences pour les bureaux d'enregistrement pourraient être évaluées, sachant qu'elles durent actuellement 5 ans. Afin d'éviter toute confusion, rien n'interdit à l'autorité d'accréditation d'exiger des documents supplémentaires lors du renouvellement de l'accréditation.

[11] Pour plus de clarté, les fournisseurs de services et/ou les avocats agissant au nom des propriétaires de marques de commerce sont également éligibles à l'accréditation. Toutefois, ces fournisseurs de services et/ou avocats agissent au nom (légalement) du propriétaire de la marque. Lorsque de tels prestataires de services et/ou avocats enfreignent les règles du SSAD, il est nécessaire que les entités divulgatrices reçoivent ces données, et il doit être clair qu'une telle violation peut être considérée dans les futures divulgations pour le propriétaire de la marque au nom duquel l'agent agit. L'utilisation de différents agents tiers ne peut pas être appliquée comme moyen d'éviter des sanctions précédentes pour une utilisation abusive du SSAD.

1.12. L'entité accréditée est censée élaborer des politiques et des procédures appropriées pour assurer une utilisation appropriée de ses informations d'identification par une personne. Chaque utilisateur doit être accrédité, mais un utilisateur agissant au nom d'une organisation doit avoir son accréditation liée à l'accréditation de son organisation.

Recommendation #2. Accréditation des entités gouvernementales

2.1. Objectif de l'accréditation

Le SSAD DOIT fournir un accès raisonnable aux données d'enregistrement aux entités qui ont besoin d'accéder à ces données pour l'exercice de leurs tâches de politique publique. Compte tenu de leurs obligations en vertu des règles de protection des données applicables, la responsabilité finale de l'octroi de l'accès aux données d'enregistrement non publiques incombera à la partie considérée comme une autorité de contrôle pour le traitement de ces données d'enregistrement qui constituent des données personnelles.

L'élaboration et la mise en œuvre d'une procédure d'accréditation qui s'applique spécifiquement aux entités gouvernementales faciliteront les décisions que les parties contractantes devront prendre avant d'accorder l'accès à des données d'enregistrement non publiques à une entité particulière ou le traitement automatisé des décisions de divulgation par le gestionnaire de la passerelle centrale, le cas échéant. Cette procédure d'accréditation peut fournir aux contrôleurs de données les informations nécessaires pour leur permettre d'évaluer et de décider de la divulgation des données.

2.2. Éligibilité

L'accréditation par l'organisme gouvernemental d'un pays ou d'un territoire ou par son organisme autorisé[12] serait mise à la disposition de diverses entités gouvernementales éligibles[13] qui ont besoin d'accéder à des données d'enregistrement non publiques pour l'exercice de leur tâche de politique publique, y compris, mais sans s'y limiter :

- Autorités chargées de l'application de la loi civile et pénale
- Protection des données et autorités règlementaires
- Autorités judiciaires
- Les organisations de défense des droits des consommateurs ont accordé une tâche de politique publique par la loi ou par délégation d'une entité gouvernementale

[12] Examen de la mise en œuvre : un tel organe pourrait être une organisation internationale gouvernementale.
[13] Les organisations intergouvernementales (OIG) sont également éligibles à l'accréditation en vertu de la Recommandation 2. Une OIG qui souhaite être accréditée DOIT demander l'accréditation par l'intermédiaire de l'autorité d'accréditation de son pays hôte.

- Les autorités de cybersécurité ont accordé une tâche de politique publique par la loi ou par délégation d'une entité gouvernementale, y compris les équipes nationales d'intervention informatique d'urgence (CERT)

2.3. Déterminer l'éligibilité

Les entités gouvernementales éligibles sont celles qui ont besoin d'accéder à des données d'enregistrement non publiques pour l'exercice de leur tâche de politique publique, conformément aux lois applicables en matière de protection des données. La question de savoir si une entité doit être éligible est déterminée par une autorité d'accréditation désignée par un pays ou territoire. Cette détermination d'éligibilité n'affecte pas la responsabilité finale de la partie contractante de déterminer s'il faut ou non divulguer des données personnelles suite à une requête de données d'enregistrement non publiques ou par le gestionnaire de la passerelle centrale dans le cas de demandes qui répondent aux critères de traitement automatisé des décisions de divulgation, le cas échéant.

2.4. Exigences de l'autorité d'accréditation gouvernementale

Les exigences relatives à l'accréditation gouvernementale DOIVENT respecter les exigences énoncées dans la Recommandation 1.3.

En outre, les exigences DOIVENT être répertoriées et mises à la disposition des entités gouvernementales éligibles. Le non-respect de ces exigences pourrait entraîner la révocation de l'accréditation de l'autorité d'accréditation par l'organisation ICANN.

2.5. Procédure d'accréditation

L'accréditation DOIT être fournie par une autorité d'accréditation approuvée. Cette autorité peut être soit l'agence gouvernementale d'un pays ou d'un territoire (par exemple, un ministère), soit déléguée à une organisation intergouvernementale. Cette autorité DEVRAIT publier les exigences relatives à l'accréditation et exécuter la procédure d'accréditation pour les entités gouvernementales éligibles.

2.5.1. L'accréditation met l'accent sur les responsabilités du demandeur de données (destinataire), qui est responsable de garantir le respect de la loi.
2.5.2. L'accréditation se concentrera sur les exigences de la loi, telles que les exigences concernant la durée de la conservation des données, le stockage sécurisé, les contrôles de données de l'organisation et les notifications de violation de données.
2.5.3. Le renouvellement, les pratiques de connexion, l'audit, les plaintes et la désaccréditation seront traités conformément à la Recommandation 1.

Orientations relatives à la mise en œuvre :

2.6. L'accréditation est requise pour qu'une entité gouvernementale puisse participer au SSAD. Les entités gouvernementales non accréditées peuvent présenter des requêtes de données en dehors du SSAD, et les parties contractantes devraient avoir des procédures en place pour fournir un accès raisonnable.
2.7. Les utilisateurs accrédités devront suivre les mesures de protection établies par la politique (consulter également de la Recommandation 11 sur les conditions d'utilisation du SSAD). Cela est sans préjudice pour l'entité de respecter les sauvegardes en vertu de son droit interne.
2.8. Les entités accréditées DEVRAIENT fournir des détails pour faciliter la décision de divulgation aux parties contractantes, comme toute loi locale applicable relative à la requête.

Recommendation #3. Critères et contenu des requêtes

3.1. L'objectif de cette recommandation est de permettre la présentation normalisée des éléments de données requis, y compris toute documentation à l'appui.

3.2. La recommandation de l'équipe responsable de l'EPDP suggère que chaque requête au SSAD DOIT inclure tous les renseignements nécessaires à une décision de divulgation, y compris les renseignements suivants :

3.2.1. Le nom de domaine relatif à la demande d'accès/divulgation ;
3.2.2. L'identification et l'information concernant le requérant, y compris l'identité et les renseignements sur l'assertion signée, tels que définis aux sections 1.4a) et 1.4b) de la Recommandation 1 ;[14]
3.2.3. Des informations sur les droits juridiques du requérant ainsi que les raisons ou justifications particulières de la requête (par exemple, la base ou le motif de la demande ; pourquoi ces données sont-elles nécessaires au requérant ?) ;
3.2.4. L'affirmation que la requête est faite de bonne foi et que les données reçues (le cas échéant) seront traitées dans le respect de la loi et uniquement en conformité avec l'objectif spécifié au point (c) ;
3.2.5. Une liste des éléments de données demandés par le requérant et la raison pour laquelle les éléments de données demandés sont nécessaires aux fins de la demande ;
3.2.6. Type de demande (par exemple, Urgente – consulter aussi la Recommandation 6, Niveaux de priorité, Confidentiel – consulter aussi la Recommandation 12, Exigences en matière de divulgation).

[14] Toutes les parties impliquées dans le SSAD devront tenir compte des exigences qui peuvent s'appliquer aux transferts transfrontaliers de données.

3.3. Le gestionnaire de la passerelle centrale[15] DOIT confirmer que toutes les informations requises soient fournies. Si le gestionnaire de la passerelle centrale détectait que la demande est incomplète, il devra en informer le demandeur en précisant les données requises manquantes et fournir au demandeur l'opportunité de compléter sa demande. Le demandeur ne pourra pas présenter une demande incomplète.

Orientations relatives à la mise en œuvre

L'équipe responsable de l'EPDP s'attend à ce que :

3.4. Chaque requête comprenne des données associées aux informations détaillées à la section 3.2 ci-dessus. Bien que le mécanisme de collecte et de placement de ces données dans une requête (qu'il s'agisse d'un formulaire Web, d'une API ou d'un outil similaire) ne soit pas spécifié par cette politique, l'offre de champs pré-remplis, de cases à cocher et/ou d'options de liste déroulante doit être prise en compte. Toutefois, l'utilisation de champs, de cases à cocher ou d'options de liste déroulante pré-remplis ne doit pas exclure la possibilité pour les requérants de donner des réponses libres.

3.5. Les requêtes doivent être rédigées en anglais sauf si la partie contractante qui reçoit la demande indique qu'elle est également disposée à recevoir la demande et/ou les documents justificatifs dans une ou plusieurs langues**.**

3.6. Une assertion signée peut fournir une ou plusieurs des exigences énumérées ci-dessus.

Recommendation #4. Accusé de réception et relais de la requête de divulgation

4.1. Accusé de réception

4.1.1. Après confirmation que la requête est syntaxiquement correcte et que tous les champs obligatoires ont été remplis, le gestionnaire de la passerelle centrale DOIT répondre immédiatement et synchroniquement avec l'accusé de réception et transmettre la demande de divulgation[16] à la partie contractante responsable.
4.1.2. La réponse fournie par le gestionnaire de la passerelle centrale au requérant DOIT également inclure des informations sur les étapes suivantes, sur la manière dont les données d'enregistrement publiques peuvent être obtenues, ainsi que sur le calendrier prévu, conformément aux SLA décrits dans la Recommandation 10.

4.2. Relais de la requête de divulgation

[15] Consulter la définition à la section 3.5.1 – Définitions.

4.2.1. Par défaut, le gestionnaire de la passerelle centrale DOIT transmettre la requête de divulgation au bureau d'enregistrement concerné. Toutefois, lorsque le gestionnaire de la passerelle centrale est au courant de toute circonstance, évaluée conformément à ces recommandations, qui nécessite la présentation d'une requête de divulgation à l'opérateur de registre concerné, le gestionnaire de la passerelle centrale POURRAIT transmettre la requête de divulgation à l'opérateur de registre concerné, à condition que les raisons qui nécessitent un tel transfert de la requête soient fournies à l'opérateur de registre pour examen. Le requérant DOIT être en mesure de signaler une telle situation au gestionnaire de la passerelle centrale, mais ce dernier DOIT faire sa propre évaluation pour déterminer si la circonstance identifiée nécessite la présentation de la requête de divulgation à l'opérateur de registre concerné. Pour plus de clarté, rien dans cette recommandation n'empêche un requérant de contacter directement, en dehors du SSAD, l'opérateur de registre concerné avec une requête de divulgation.

Orientations relatives à la mise en œuvre

L'équipe responsable de l'EPDP s'attend à ce que :

4.3. L'accusé de réception comprenne un « numéro de ticket » ou un mécanisme similaire pour faciliter les interactions entre le requérant et le SSAD, dont les détails seront précisés lors de la mise en œuvre.
4.4. Le gestionnaire de la passerelle centrale transmette la requête de divulgation ainsi que les informations nécessaires et appropriées concernant le requérant à la partie contractante. S'il s'agit d'une requête de divulgation pour laquelle le traitement automatisé de la décision de divulgation est applicable (consulter la recommandation Automatisation), le relais de la requête de divulgation et de toutes les informations pertinentes peut se produire en même temps que le gestionnaire de la passerelle centrale demande à la partie contractante de divulguer automatiquement au requérant les données demandées.

Recommendation #5. Exigences de réponse

5.1. Pour le gestionnaire de la passerelle centrale :[17]
5.1.1. Dans le cadre de son relais à la partie contractante responsable, le gestionnaire de la passerelle centrale POURRAIT fournir une recommandation de faire ou non la divulgation à la partie contractante.

5.2. Pour les parties contractantes :

[17] Veuillez noter que les exigences relatives aux requêtes de divulgation qui répondent aux critères des décisions de divulgation automatisée sont couvertes dans la Recommandation 9.

5.2.1. La partie contractante POURRAIT suivre la recommandation du gestionnaire de la passerelle centrale, mais elle n'est pas tenue de le faire. Si la partie contractante décidait de ne pas suivre la recommandation du gestionnaire de la passerelle centrale, elle DOIT communiquer ses raisons au gestionnaire de la passerelle centrale afin que ce dernier puisse en tirer une leçon et améliorer les recommandations de réponses futures.

5.2.2. La partie contractante DOIT fournir une réponse de divulgation sans retard indu, sauf dans des circonstances exceptionnelles. Ces circonstances exceptionnelles POURRAIENT inclure le nombre total de requêtes reçues si le nombre dépasse de loin les SLA établis.[18] Les requêtes du SSAD qui répondent aux critères de réponse automatique doivent recevoir une réponse de divulgation automatique. Pour les requêtes qui ne répondent pas aux critères de réponse automatique, une réponse DOIT être reçue conformément aux SLA décrits dans la recommandation de SLA.

5.2.3. Lorsque la divulgation des données (en tout ou en partie) a été refusée, les réponses DOIVENT comprendre des justifications suffisantes pour permettre au demandeur de comprendre objectivement les raisons du refus, y compris, par exemple, une analyse et une explication de la façon dont le test d'équilibrage a été appliqué (le cas échéant)[19]. En outre, dans sa réponse, la partie contractante POURRAIT inclure des informations sur la façon dont les données d'enregistrement public peuvent être obtenues.

5.2.4. Si la partie contractante déterminait que la divulgation constituerait une violation des lois applicables ou entraînerait une incohérence avec les présentes recommandations de politique, la partie contractante DEVRA documenter le fondement et communiquer ces informations au requérant et, si nécessaire, à l'organisation ICANN.

5.3. Si un requérant est d'avis que sa requête a été refusée en violation des exigences procédurales de cette politique, une plainte POURRAIT être déposée auprès de l'organisation ICANN. L'organisation ICANN DOIT enquêter sur les plaintes concernant les requêtes de divulgation dans le cadre de ses processus d'application.

5.4. L'organisation ICANN DOIT mettre à disposition un mécanisme d'alerte par lequel tant les requérants que les personnes concernées dont les données ont été divulguées peuvent alerter l'organisation ICANN s'ils sont d'avis que la divulgation ou la non-divulgation sont le résultat d'un abus systémique par une partie contractante. Ce mécanisme d'alerte n'est pas un mécanisme de recours (pour contester la divulgation ou la non-divulgation, les parties concernées sont censées utiliser les mécanismes de règlement de litiges disponibles tels que les tribunaux ou les autorités de protection des données) mais il devrait aider à informer le service de la conformité de l'ICANN des

[18] Consulter la Recommandation 12 pour de plus amples détails sur ce qui est considéré comme une utilisation abusive du SSAD.

[19] Conformément à la Recommandation 6, il convient de veiller à ce qu'aucune donnée personnelle ne soit révélée au requérant dans cette explication.

allégations de non-respect systémique des exigences de cette politique, qui doivent déclencher une action d'application de la loi appropriée.

Orientations relatives à la mise en œuvre

5.5. L'information résultant du mécanisme d'alerte devrait également être incluse dans le rapport sur l'état d'avancement de la mise en œuvre du SSAD (consulter la Recommandation 18) afin de permettre un examen plus approfondi des mesures correctives possibles pour remédier aux comportements abusifs.

5.6. L'équipe responsable de l'EPDP ne s'attend pas à ce que le gestionnaire de la passerelle centrale fournisse une recommandation dès le premier jour car il est entendu que l'expérience devra être acquise avant que le gestionnaire de la passerelle centrale puisse être en mesure de fournir une telle recommandation à la partie contractante. Il est prévu qu'une recommandation soit élaborée de manière automatisée en tenant compte des informations contenues dans la requête, des informations sur le requérant et de l'historique des requêtes du requérant.

Recommendation #6. Niveaux de priorité

6.1. L'équipe responsable de l'EPDP recommande que le gestionnaire de la passerelle centrale accepte au moins les trois (3) niveaux de priorité suivants, parmi lesquels le requérant peut choisir lorsqu'il soumet des requêtes via le SSAD. Le niveau de priorité définit l'urgence avec laquelle la requête de divulgation doit être traitée par la partie contractante :

6.1.1. **Priorité 1** - Requêtes urgentes - Les critères de détermination des requêtes urgentes se limitent aux circonstances qui constituent une menace imminente à la vie, des blessures graves, des infrastructures critiques (en ligne et hors ligne) ou l'exploitation des enfants. Afin d'éviter toute confusion, la priorité 1 ne se limite pas aux requêtes des organismes d'application de la loi.

6.1.2. **Priorité 2** - procédures administratives de l'ICANN - requêtes de divulgation qui sont le résultat de procédures administratives en vertu des conditions contractuelles de l'ICANN ou des politiques de consensus existantes, telles que les demandes de vérification UDRP et URS.[20]

6.1.3. **Priorité 3** - toutes les autres demandes.

6.2. Pour les requêtes de priorité 3, les requérants DOIVENT être en mesure d'indiquer que la requête de divulgation concerne un problème de protection des consommateurs (hameçonnage, logiciel malveillant ou fraude), auquel cas la partie

[20] Pour plus de clarté, cette attribution de priorité devrait être limitée aux fournisseurs de services de règlement de litiges approuvés par l'ICANN ou à ses employés dans le cadre des procédures administratives de l'ICANN.

contractante DEVRAIT donner la priorité à la requête par-dessus les autres requêtes de priorité 3. Un abus persistant de cette indication peut entraîner la désaccréditation du requérant.

6.3. La partie contractante :

- POURRAIT réaffecter le niveau de priorité au cours de l'examen de la requête. Par exemple, lorsqu'une requête est examinée manuellement, la partie contractante POURRAIT noter que, bien que la priorité soit définie comme « priorité 2 » (procédure administrative de l'ICANN), la requête ne présente aucune preuve documentant une procédure administrative de l'ICANN telle qu'un cas UDRP classé et, en conséquence, la requête devrait être recatégorisée comme de « priorité 3 ».
- DOIT communiquer tout nouveau classement de la priorité de la requête au gestionnaire de la passerelle centrale et au requérant.

6.4. La recommandation de l'équipe responsable de l'EPDP suggère que le SSAD DOIT appuyer les requêtes de divulgation « urgente » du SSAD auxquelles s'appliquent les exigences suivantes :

6.4.1. Abus de requêtes urgentes : les violations de l'utilisation des requêtes SSAD urgentes résulteront en une réponse du gestionnaire de la passerelle centrale pour s'assurer que les exigences relatives aux requêtes SSAD urgentes soient, en premier lieu, connues et satisfaites. Toutefois, des violations répétées peuvent empêcher le gestionnaire de la passerelle centrale de faire des requêtes urgentes via le SSAD.

6.4.2. Les parties contractantes DOIVENT maintenir un contact dédié pour traiter les requêtes SSAD urgentes qui peuvent être stockées et utilisées par le gestionnaire de la passerelle centrale, aux cas où une requête SSAD aurait été signalée comme urgente.

6.5. La recommandation de l'équipe responsable de l'EPDP suggère que les parties contractantes DOIVENT publier leur heure de travail normalisées, leurs jours ouvrables et leur fuseau horaire dans le portail du SSAD.

Orientations relatives à la mise en œuvre

6.6 Consulter, pour référence le Cadre des mesures à mettre en œuvre par les opérateurs de registre pour répondre à des menaces à la sécurité , qui signale que : « *La catégorisation initiale d'une requête comme étant de « priorité élevée » devrait être évidente et ne devrait nécessiter aucune compétence particulière pour déterminer un lien avec la sécurité publique. La « priorité élevée » devrait être considérée comme une menace imminente à la vie humaine, aux infrastructures essentielles ou à l'exploitation des enfants ».*

6.7 « Infrastructures critiques » fait allusion aux systèmes physiques et cybernétiques essentiels du fait que leur incapacité ou leur destruction aurait un impact négatif majeur sur la sécurité physique ou économique ou sur la santé ou la sécurité publique.

6.8 Consulter aussi la Recommandation 10 qui contient de plus amples détails sur les exigences relatives à une requête urgente du SSAD.

Comment la priorité est-elle définie ?
La priorité est un code attribué aux requêtes de divulgation qui suppose que le traitement se fera sur la base des délais de réponse ciblés accordés au mieux des efforts.

Qui définit la priorité ?
La priorité initiale d'une requête de divulgation est définie par le requérant, à l'aide des options de priorité définies par la présente politique. Lors de la sélection d'une priorité, le gestionnaire de la passerelle centrale indique clairement les critères applicables à une demande urgente et les conséquences potentielles de l'abus de ce paramètre de priorité.

Que se passe-t-il si la priorité doit être modifiée ?
Il est possible que la priorité définie initialement soit réaffectée lors de la révision de la requête. Par exemple, lorsqu'une requête est examinée manuellement, la partie contractante PEUT noter que, bien que la priorité soit définie comme « priorité 2 » (UDRP/URS), la requête ne présente aucune preuve documentant une procédure telle qu'un cas UDRP classé et, en conséquence, la requête devrait être reclassée comme de « priorité 3 ». Tout reclassement DOIT être communiqué au gestionnaire de la passerelle centrale et au requérant. Après réception d'une requête de divulgation non automatisée du gestionnaire de la passerelle centrale, la partie contractante est responsable de déterminer si les données non publiques doivent être divulguées. La partie contractante DOIT répondre à la requête dans les délais de réponse définis ci-dessus.

Recommendation #7. Finalités du requérant

7.1. L'équipe responsable de l'EPDP recommande ce qui suit :

7.1.1. Les requérants DOIVENT soumettre des requêtes de divulgation de données à des finalités spécifiques, notamment, mais sans s'y limiter : (i) l'application de la loi pénale, la sécurité nationale ou publique, (ii) les enquêtes non policières et les réclamations civiles, y compris les réclamations en matière de violation de la propriété intellectuelle et les réclamations UDRP et URS, (iii) la protection des consommateurs, la

prévention des abus et la sécurité du réseau et (iv) les obligations applicables aux entités réglementées.[21] Les requérants POURRAIENT également soumettre des requêtes de vérification de données sur la base du consentement du titulaire de nom enregistré (RNH) qui a été obtenu par le requérant (et qui est sous la seule responsabilité de ce demandeur), par exemple pour valider la réclamation de propriété du titulaire de nom enregistré concernant un enregistrement de nom de domaine, ou un contrat avec le requérant.

7.1.2. L'affirmation de l'une de ces finalités spécifiques ne garantit pas l'accès dans tous les cas, mais dépendra de l'évaluation du bien-fondé de la demande spécifique, du respect de toutes les exigences politiques applicables et de la base juridique de la requête.

Recommendation #8. Autorisation des parties contractantes.

Pour plus de clarté, cette recommandation concerne les requêtes de divulgation qui sont acheminées à la partie contractante pour examen. Ces exigences NE s'appliquent PAS aux requêtes de divulgation qui répondent aux critères de traitement automatisé des décisions de divulgation décrits dans la Recommandation 9, peu importe si le traitement automatisé des décisions de divulgation est obligatoire ou à la demande de la partie contractante. La présente recommandation ne remplace pas la possibilité pour les parties contractantes de faire la distinction entre les titulaires de noms de domaine selon leur situation géographique, comme cela est stipulé à la Recommandation 16 (de l'étape 1 de l'EPDP), ni la possibilité pour les parties contractantes de faire la distinction entre les personnes morales et les personnes physiques conformément à la Recommandation 17 (de l'étape 1 de l'EPDP) pour cette recommandation spécifique.

Exigences générales

La partie contractante

8.1. DOIT examiner chaque requête individuellement et pas en masse, peu importe si la révision est effectuée automatiquement ou à travers un examen approfondi et NE DOIT PAS divulguer de données uniquement sur la base de la catégorie d'utilisateurs accrédités.

8.2. POURRAIT externaliser la responsabilité de l'autorisation à un fournisseur tiers, mais la partie contractante restera responsable, en dernier ressort, de s'assurer que les exigences applicables soient respectées.

[21] Par exemple, la directive de l'UE sur la sécurité des réseaux et des systèmes d'information (connue sous le nom de directive NIS) impose des obligations spécifiques aux fournisseurs de services numériques et aux opérateurs de services essentiels.

8.3. DOIT déterminer sa propre base légale pour le traitement lié à la décision de divulgation.[22] Le requérant aura la possibilité d'identifier la base légale selon laquelle il s'attend à ce que la partie contractante divulgue les données demandées ; toutefois, dans tous les cas où la partie contractante est chargée de prendre la décision de divulguer, la partie contractante DOIT prendre la décision finale de la base légale appropriée.

8.4. DOIT prendre en charge les requêtes de réexamen reçues via le système SSAD et DOIT les prendre en compte en fonction de la justification fournie par le requérant. Pour plus de clarté, la nouvelle soumission d'une requête de divulgation identique à la requête initiale, sans fondement justifiant la raison pour laquelle la requête doit être réexaminée, n'a pas besoin d'être réexaminée par la partie contractante.

8.5. En l'absence de toute obligation légale contraire, la divulgation NE DOIT PAS être refusée uniquement par manque de l'un des éléments suivants : (i) une ordonnance du tribunal ; (ii) une citation à comparaître ; (iii) une action civile en attente ; ou (iv) une procédure UDRP ou URS ; de même, une divulgation ne peut pas être refusée uniquement en raison du fait que la requête soit fondée sur une violation prétendue à la propriété intellectuelle.

Exigences de détermination de l'autorisation

Suite à la réception d'une requête du gestionnaire de la passerelle centrale, la partie contractante :

8.6. DOIT procéder à un examen prima facie[23] de la validité de la requête, c'est-à-dire que la requête suffit pour permettre à la partie contractante de procéder à un examen de fond et de traiter les données sous-jacentes associées. Si la partie contractante déterminait que la requête n'est pas valide, par exemple si elle ne fournissait pas un motif suffisant pour une révision de fond des données sous-jacentes, la partie contractante DEVRA demander au requérant de fournir des informations supplémentaires avant de refuser la requête ;

8.7. Si la requête était jugée valide à la suite de l'examen prima facie, la partie contractante DEVRA procéder à une révision de fond de la requête et des données sous-jacentes :

8.7.1. Si, suite à l'évaluation des données sous-jacentes, la partie contractante déterminait raisonnablement que la divulgation des éléments de données demandés n'entraînerait pas la divulgation des données personnelles, la partie contractante DEVRA divulguer les données, à moins que la divulgation ne

[22] Consulter également le point 17 des orientations de mise en œuvre.

[23] Selon le Dictionnaire de Cambridge, à première vue (basé sur ce qui semble être la vérité lorsqu'on le voit ou l'entend pour la première fois).

soit interdite par la loi applicable.[24] Pour plus de clarté, si la divulgation n'entraîne pas la divulgation de données personnelles, la partie contractante n'est pas censée poursuivre l'évaluation de la demande.

8.7.2. Si, suite à l'évaluation des données sous-jacentes, la partie contractante déterminait que la divulgation des éléments de données requis entraînerait la divulgation des données personnelles, la partie contractante DEVRA déterminer, au minimum, dans le cadre de sa révision de fond et les données sous-jacentes :

8.7.2.1. Si la partie contractante dispose d'une base légale pour la divulgation ;[25]

8.7.2.2. Si tous les éléments de données requis sont nécessaires ;[26]

8.7.2.3. La question de savoir si un équilibrage ou une révision sont requis conformément à la base légale identifiée par la partie contractante comme dans 8.3.

8.8. Si la requête fait l'objet d'un équilibrage ou d'un réexamen conformément au paragraphe 8.7.2.3 :

8.8.1. DEVRA divulguer les données si, sur la base de son évaluation, la partie contractante déterminait que l'intérêt légitime du requérant n'est pas compensé par les intérêts ou les droits et libertés fondamentaux de la personne concernée. La partie contractante DEVRA documenter le fondement de son approbation.

8.8.2. DEVRA refuser la requête si, sur la base de son évaluation, la partie contractante déterminait que l'intérêt légitime du demandeur serait compensé par les intérêts ou les droits et libertés fondamentaux de la personne concernée. La partie contractante DEVRA documenter la raison de son refus et DEVRA communiquer la raison du refus au gestionnaire de la passerelle centrale, en veillant à ce qu'aucune donnée personnelle ne soit incluse dans le fondement du refus.

8.9. Si la requête ne faisait pas l'objet d'un équilibrage ou d'un réexamen conformément au paragraphe 8.7.2.3 :

8.9.1. DEVRA divulguer si la partie contractante déterminait qu'elle a une base légale ou n'est pas interdite de divulguer des données en vertu de la loi applicable. La partie contractante DEVRA documenter le fondement de son approbation.

[24] Lors de l'examen de la publication de données non publiques de personnes morales, en particulier en ce qui concerne les ONG et les parties engagées dans des activités en matière de droits de l'homme qui peuvent être protégées par le droit local (par exemple le Droit constitutionnel et le Droit de la Charte), la partie contractante devrait examiner l'impact sur les personnes physiques qui pourraient être potentiellement identifiées à travers la divulgation des données de la personne morale.

[25] Consulter également le point 17 des orientations de mise en œuvre

[26] Pour un contexte plus approfondi concernant la définition de « nécessaire », veuillez vous reporter à la page 7 des directives juridiques auxquelles l'équipe responsable de l'EPDP a fait référence lors de la formulation de cette définition.

8.9.2. DEVRA refuser la demande si la partie contractante déterminait qu'elle n'a pas de base légale ou qu'elle est interdite de divulguer des données en vertu de la loi applicable. La partie contractante DEVRA documenter la raison de son refus et DEVRA communiquer la raison du refus au gestionnaire de la passerelle centrale, en veillant à ce qu'aucune donnée personnelle ne soit incluse dans le fondement du refus.

Le requérant :

8.10. POURRAIT déposer une demande de réexamen s'il croyait que sa requête a été refusée de façon incorrecte.

8.11. DEVRA, dans le cadre de sa demande de réexamen, justifier la raison pour laquelle sa requête doit être réexaminée. La justification doit fournir suffisamment de détails sur les raisons pour lesquelles le requérant estime que sa requête a été refusée de façon incorrecte.

8.12. Si un requérant croyait qu'une partie contractante ne se conforme à aucune des exigences de la présente politique, le demandeur DEVRAIT en aviser l'organisation ICANN en fonction du mécanisme d'alerte décrit dans la Recommandation 5, Exigences de réponse.

Orientations relatives à la mise en œuvre

8.13. L'équipe responsable de l'EPDP envisage que la partie contractante ait la possibilité de communiquer avec le requérant via un ticket dédié dans le SSAD. L'équipe responsable de l'EPDP envisage également que le SSAD soit entièrement protégé par une technologie de protection des données conforme aux normes de l'industrie, y compris le chiffrement pour protéger la transmission des données personnelles, conformément aux lois sur la protection des données et sur la cybersécurité applicables.

8.14. L'équipe responsable de l'EPDP note les détails de la façon dont la communication au paragraphe 8.6 sera évaluée au cours de l'étape de mise en œuvre de la politique ; toutefois, l'équipe responsable de l'EPDP fournit cette orientation supplémentaire à titre d'assistance. L'équipe responsable de l'EPDP envisage que la partie contractante envoie un avis au requérant, via le ticket SSAD approprié, notant sa décision de refuser la requête. Le requérant dispose alors de (x) jours pour fournir des informations mises à jour à la partie contractante. Lorsque le requérant fournit des informations mises à jour, le temps de réponse du SLA serait réinitialisé. Par exemple, la partie contractante dispose d'un jour ouvrable pour répondre à la demande urgente mise à jour. Si le requérant choisissait de ne pas fournir les informations, le SLA sera compté à partir du moment où la partie contractante enverra l'avis d'« intention de

refuser » au requérant. Si le requérant décidait de ne pas répondre, la requête sera refusée dès l'expiration du délai.

8.15. Dans les situations où la partie contractante évalue l'intérêt légitime du requérant, la partie contractante DOIT tenir compte des éléments suivants :

8.15.1. L'intérêt doit être spécifique, réel et présent plutôt que vague et spéculatif.

8.15.2. Un intérêt est généralement considéré comme légitime pour autant qu'il puisse être poursuivi conformément à la protection des données et à d'autres lois.

8.15.3. Les exemples d'intérêts légitimes comprennent : (i) l'application, l'exercice ou la défense de poursuites judiciaires, y compris la violation de la propriété intellectuelle ; (ii) la prévention de la fraude et de l'utilisation abusive des services ; (iii) la sécurité physique, informatique et de réseau.

8.16. Dans le cadre de sa révision de fond, la partie contractante DEVRAIT évaluer, au moins :

8.16.1. Le cas échéant, les facteurs suivants devraient être utilisés pour déterminer si l'intérêt légitime du requérant n'est pas compensé par les intérêts ou les droits et libertés fondamentaux de la personne concernée. Aucun facteur unique n'est déterminant ; au lieu de cela, la partie contractante DEVRAIT considérer l'ensemble des circonstances décrites ci-dessous :

8.16.1.1. *Évaluation de l'impact*. Tenir compte de l'impact direct sur les personnes concernées ainsi que de toutes les conséquences plus générales possibles du traitement des données. Tenir compte de l'intérêt public et des intérêts légitimes poursuivis par le requérant pour, par exemple, maintenir la sécurité et la stabilité du DNS.

Chaque fois que les circonstances de la requête de divulgation ou la nature des données à divulguer suggèrent un risque accru pour la personne concernée, cela devra être pris en compte lors de la prise de décision.

8.16.1.2. *Nature des données.* Évaluer le niveau de sensibilité des données et de la question de savoir si les données sont déjà accessibles au public.

8.16.1.3. *Statut de la personne concernée.* Déterminer si le statut de la personne concernée augmente sa vulnérabilité (par exemple, les enfants, les demandeurs d'asile, les autres classes protégées)

8.16.1.4. *Portée du traitement.* Tenir compte des informations issues de la requête de divulgation ou d'autres circonstances pertinentes qui indiquent si les données seront conservées en toute sécurité (risque plus faible) par rapport à des informations publiques, rendues accessibles à un grand nombre de personnes, ou combinées à

d'autres données (risque plus élevé),[27] à condition que cela ne soit pas destiné à interdire les divulgations publiques pour des actions en justice ou des procédures administratives de règlement de litiges comme l'UDRP ou l'URS.

8.16.1.5. *Attentes raisonnables de la personne concernée.* Déterminer si la personne concernée s'attend raisonnablement à ce que ses données soient traitées/divulguées de cette manière.

8.16.1.6. *Statut de l'autorité de contrôle et de la personne concernée.* Tenir compte du pouvoir de négociation et de tout déséquilibre d'autorité entre l'autorité de contrôle et la personne concernée.[28]

8.16.1.7. *Cadres juridiques concernés.* Tenir compte des cadres juridiques juridictionnels du demandeur, des parties contractantes et de la personne concernée, et de la manière dont cela peut affecter les divulgations potentielles.

8.16.1.8. *Transferts transfrontaliers de données.* Tenir compte des exigences qui peuvent s'appliquer aux transferts transfrontaliers de données.

8.17. Dans ce cas particulier, une base légale à ces effets peut être basée sur la présence d'une base légale en vertu de la politique de l'ICANN (ou de la loi applicable).

L'application du test d'équilibrage et des facteurs considérés dans la présente section DEVRAIT être révisée, le cas échéant, pour traiter de la jurisprudence applicable interprétant le RGPD, des lignes directrices émises par le CEPD ou des révisions du RGPD ou d'autres lois applicables en matière de vie privée qui pourraient se produire à l'avenir.

Recommendation #9. Automatisation du traitement SSAD

9.1. La recommandation de l'équipe responsable de l'EPDP suggère que le gestionnaire de la passerelle centrale DOIT automatiser la réception, l'authentification et la transmission des demandes SSAD à la partie contractante concernée dans la mesure où cela serait techniquement et commercialement faisable et légalement autorisé.

[27] Pour plus de contexte concernant la définition de « risque plus élevé » lorsque les données sont combinées, veuillez vous reporter à la page 5 des directives juridiques auxquelles l'équipe responsable de l'EPDP a fait référence lors de la formulation de cette définition.

[28] Dans le cadre de l'autorisation de la partie contractante, les parties concernées sont la partie contractante (autorité de contrôle) et le titulaire de nom de domaine (personne concernée) ; toutefois, les rôles et responsabilités des parties seront abordés plus en détail lors de la mise en œuvre.

9.2. Le SSAD DOIT permettre l'automatisation du traitement des demandes bien formées, valides, complètes et correctement identifiées des utilisateurs accrédités comme décrit ci-dessous.

Traitement automatisé des décisions de divulgation

9.3. Les parties contractantes DOIVENT traiter de manière automatisée les décisions de divulgation pour toutes les catégories de demandes pour lesquelles l'automatisation est déterminée (consulter le point 9.4 et les processus détaillés dans la Recommandation 18) pour être techniquement et commercialement[29] réalisables[30] et juridiquement admissibles. Afin d'éviter toute confusion, l'équipe responsable de l'EPDP recommande que toutes les catégories de décisions de divulgation qui ne répondent pas actuellement à ces critères ne soient pas saisies à l'avenir, sous réserve des processus détaillés dans la Recommandation 18. Dans les domaines où les décisions de divulgation ne répondent pas à ces critères, la normalisation du processus décisionnel en matière de divulgation est l'objectif de base.

9.4. Selon les directives juridiques obtenues (consulter l'avis sur les cas d'utilisation de re-automatisation dans le contexte de la divulgation des données non publiques des titulaires de noms de domaine - avril 2020), l'équipe responsable de l'EPDP recommande que les types suivants de demandes de divulgation, pour lesquels la recevabilité juridique a été indiquée dans le RGPD pour l'automatisation complète (réception et traitement de la décision de divulgation) DOIT être automatisé à partir du moment du lancement du SSAD :

- 9.4.1. Les demandes de l'application de la loi dans les juridictions locales ou autrement applicables avec 1) une base juridique confirmée du RGPD 6(1)e ou 2) le traitement doit être effectué en vertu d'une exemption de l'article 2 du RGPD ;
- 9.4.2. L'enquête sur une violation de la législation sur la protection des données prétendument commise par l'ICANN/les parties contractantes affectant le titulaire de nom de domaine ;
- 9.4.3. La demande pour le champ « ville » uniquement, pour évaluer s'il faut poursuivre une réclamation ou si cela ne répond qu'à des fins statistiques ;
- 9.4.4. Aucune donnée personnelle sur le dossier d'enregistrement ayant été précédemment divulguée par la partie contractante.

[29] Pendant la mise en œuvre, il faudra examiner plus en profondeur la faisabilité commerciale pour les bureaux d'enregistrement qui peuvent recevoir un nombre très limité de demandes satisfaisant aux critères de traitement automatisé des décisions de divulgation et si la charge financière de permettre ce traitement automatisé était d'une telle nature qu'une exemption pourrait s'avérer nécessaire. Dans le cadre de cette considération, le gestionnaire de la passerelle centrale devrait également examiner comment il peut faciliter l'intégration du système d'une partie contractante avec le SSAD afin de réduire toute charge potentielle de traitement automatisé des décisions de divulgation.

[30] L'examen initial de la viabilité financière de l'automatisation sera abordé par l'organisation ICANN avec l'équipe de révision de la mise en œuvre et par la suite par le mécanisme pour l'évolution du SSAD, le cas échéant.

9.5. Pour plus de clarté, si une partie contractante déterminait que le traitement automatisé des décisions de divulgation pour les cas d'utilisation spécifiés dans la présente recommandation ou par le biais des processus détaillés dans la Recommandation 18 n'est pas juridiquement admissible ou comporte un risque important n'ayant pas été reconnu dans les directives juridiques obtenues par l'équipe responsable de l'EPDP mais ayant été identifié et documenté par la suite, par exemple, par une évaluation de l'impact sur la protection des données (DPIA), la partie contractante DOIT notifier l'organisation ICANN du besoin d'une exemption, du traitement automatisé des décisions de divulgation pour le ou les cas d'utilisation identifié(s) et DOIT inclure la documentation à l'appui avec son avis. Les notifications d'exemption déraisonnables POURRAIENT faire l'objet d'un examen par l'organisation ICANN. L'organisation ICANN DOIT annuler la reconnaissance d'exemption si elle trouve que la notification de la partie contractante est incorrecte ou abusive.

9.6. Dès que l'organisation ICANN a été notifiée, le gestionnaire de la passerelle centrale DOIT interrompre la transmission des cas d'utilisation identifiés comme nécessitant un traitement automatisé et DOIT transmettre la requête conformément aux exigences de la Recommandation 8 – Autorisation de la partie contractante.

9.7. L'organisation ICANN DOIT fournir un processus de notification et de commentaires pour permettre aux parties prenantes concernées de présenter des commentaires sur les exemptions prévues au paragraphe 9.5. L'organisation ICANN POURRAIT faciliter une discussion ultérieure entre les parties prenantes concernées et la partie contractante en question afin de faciliter la compréhension mutuelle de l'exemption et des informations complémentaires. D'autres détails seront déterminés dans la mise en œuvre, y compris la confidentialité potentielle du processus.

9.8. Dès que la partie contractante prend conscience que l'exemption n'est plus applicable, elle DOIT en informer l'organisation ICANN en conséquence.

9.9. À la suite de la notification d'une partie contractante en vertu du paragraphe 9.8, le responsable de la passerelle centrale DOIT transmettre à la partie contractante les requêtes qui répondent aux critères de traitement automatisé conformément à la présente recommandation et la partie contractante DOIT reprendre le traitement automatisé des décisions de divulgation pour les cas d'utilisation pertinents.

9.10. En ce qui concerne les demandes de divulgation qui seraient envoyées à une partie contractante pour examen, une partie contractante POURRAIT demander à la passerelle centrale d'automatiser le traitement de la décision de divulgation de tous ou certains types de requêtes de divulgation et/ou de requêtes provenant d'un

requérant donné,[31] après que la partie contractante aura évalué le risque et l'admissibilité juridique, selon le cas.

9.11. Une partie contractante POURRAIT, à tout moment, retirer ou réviser une demande d'automatisation de la décision de divulgation qui n'est pas requise par les présentes recommandations de politique.

9.12. Pour plus de clarté, le gestionnaire de la passerelle centrale surveille si une requête de divulgation répond aux critères de traitement automatisé des décisions de divulgation qui POURRAIENT impliquer une révision non automatisée à la passerelle centrale. De même, la passerelle centrale POURRAIT demander à la partie contractante des renseignements supplémentaires qui pourraient aider le gestionnaire de la passerelle centrale à déterminer si les critères d'un traitement automatisé des décisions de divulgation ont été remplis ou non. Une partie contractante POURRAIT fournir ces informations supplémentaires, si nécessaire. Il n'est pas prévu que les données personnelles soient transférées en réponse à une telle requête d'information.

Orientations relatives à la mise en œuvre

En plus des exigences détaillées dans la Recommandation 4 (accusé de réception) et la Recommandation 10 (SLA), ce qui s'appliquera également au traitement automatisé des décisions de divulgation, les directives de mise en œuvre suivantes s'appliqueront au traitement automatisé des décisions de divulgation, c'est-à-dire les requêtes pour lesquelles le gestionnaire de la passerelle centrale détermine qu'une décision automatisée de la partie contractante à la requête de divulgation est nécessaire, conformément à la présente recommandation.

9.13. L'équipe responsable de l'EPDP s'attend à ce que les aspects du SSAD tels que la réception des requêtes, la vérification des données d'identification, la validation de la soumission des requêtes (le format et l'exhaustivité, pas le contenu) puissent être automatisées, bien qu'il ne soit probablement pas possible d'automatiser complètement tous les aspects de la révision de la requête de divulgation dans tous les cas.

9.14. Dans le contexte de la poursuite de l'examen des cas d'utilisation potentiels jugés juridiquement admissibles dans le cadre de la Recommandation 18, en l'absence de directives faisant autorité (par exemple, le CEPD, la Cour de justice de l'Union européenne (CJCE), la nouvelle loi), le droit applicable devra être déterminé par la ou les parties responsables du traitement automatisé des décisions de divulgation.

[31] Par exemple, une partie contractante pourrait envisager de mettre en œuvre un système de notification de confiance qui permettrait de qualifier les requérants qui répondent à certains critères établis par la partie contractante concernée pour obtenir des réponses automatisées à leurs demandes de divulgation.

9.15. À la suite de l'orientation juridique mentionnée ci-dessus, l'équipe responsable de l'EPDP recommande que, dans sa révision, le Comité permanent de la GNSO (consulter la Recommandation 18) examine les sauvegardes énoncées à l'annexe 2 de l'Avis sur les cas d'utilisation de la ré-automatisation dans le contexte de la divulgation des données non publiques des titulaires de noms de domaine (avril 2020) et les cas d'utilisation décrits à la section 3.4 de cet avis pour déterminer si la divulgation constituerait un effet juridique ou tout aussi significatif, ce qui pourrait empêcher l'automatisation de la divulgation.

9.16. Le manière dont le traitement automatisé des décisions de divulgation est censé fonctionner dans la pratique serait que le gestionnaire de la passerelle centrale confirmerait que la requête satisfait aux exigences du traitement automatisé et exigerait à la partie contractante de divulguer automatiquement les données demandées au requérant. Le mécanisme devrait être déterminé au cours de la mise en œuvre.

9.17. Toutes les parties impliquées dans le SSAD devront tenir compte des exigences qui peuvent s'appliquer aux transferts transfrontaliers de données.

Recommendation #10. Détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD

10.1. L'équipe responsable de l'EPDP recommande aux parties contractantes de respecter les conventions de service (SLA) élaborées, mises en œuvre, appliquées et mises à jour de temps à autre conformément à la Recommandation 18, en vertu des directives de mise en œuvre fournies ci-dessous.

10.2. Aux fins du calcul du temps de réponse du SLA, l'équipe responsable de l'EPDP recommande que le SLA commence lorsqu'une requête validée avec toutes les informations de support soit fournie à la partie contractante par le gestionnaire de la passerelle centrale et s'arrête lorsque la partie contractante répond (via la passerelle centrale) avec les informations requises, une réponse de rejet ou une requête d'informations supplémentaires. Une demande de réexamen ou une réponse du requérant contenant plus d'informations serait considérée comme le début d'une nouvelle requête aux fins du calcul de la SLA.

Matrice de priorité pour les requêtes de divulgation non automatisées

Type de requête	Priorité	SLA proposé[32] (Conformité à 6 mois / 12 mois / 18 mois)

[32] Remarque : les jours ouvrables mentionnés dans le tableau sont à compter du moment où la partie contractante reçoit la requête de divulgation du gestionnaire de la passerelle centrale.

Requêtes urgentes	1	1 jour ouvrable, ne doit pas dépasser 3 jours civils (85 % / 90 % / 95 %)
Procédures administratives de l'ICANN	2	Max. 2 jours ouvrables (85 % / 90 % / 95 %)
Toutes les autres demandes*	3	Consulter les directives de mise en œuvre ci-dessous.

*Remarque : rien dans ces recommandations n'interdit explicitement le développement de nouvelles catégories et de SLA définis.

Orientations relatives à la mise en œuvre

10.3. Les exigences relatives aux priorités 1 et 2 sont censées être rendues obligatoires par le document de politique de consensus. Les exigences de niveau de service de priorité 3 peuvent également être contraignantes dans le cadre du document de politique de consensus, en consultation avec l'IRT.

Définitions proposées

Jour ouvrable :[33] tel que défini dans la juridiction de la partie contractante.
Temps de réponse moyen : Moyenne mobile de tous les temps de réponse, calculée automatiquement fréquemment (par exemple au quotidien ou une fois par semaine) comme un moyen pour qu'une partie contractante puisse évaluer ses propres performances à tout moment.
Intervalle d'évaluation du temps de réponse cible Une période de 3 mois permettant d'examiner la performance du temps de réponse 4 fois par an.
Valeur de réponse cible : La valeur de la mesure du temps de réponse moyen le jour de clôture de l'intervalle d'évaluation de la valeur de réponse cible.
Valeur de réponse cible : La même définition que pour la valeur de réponse cible, mais y ajoutant une révision de la conformité avec cette cible de la SLA.

Les exigences de temps de réponse de la partie contractante pour les demandes SSAD seront échelonnées en deux étapes :

- l'étape 1 commence **six (6) mois** après la date d'entrée en vigueur de la politique du SSAD.
- l'étape 2 commence **un (1) an** après la date d'entrée en vigueur de la politique du SSAD.

ÉTAPE 1 (s'applique uniquement aux requêtes de priorité 3)

[33] Consulter aussi la Recommandation 6.5

10.4. Au cours de l'étape 1, et en continuant par la suite, les cibles de réponse de la partie contractante pour les requêtes de priorité 3 du SSAD seront de cinq (5) jours ouvrables.

10.5. Le gestionnaire de la passerelle centrale DOIT mesurer les cibles de réponse à l'aide d'un temps de réponse moyen, et non individuellement par réponse.

10.6. Le SSAD DOIT calculer le temps de réponse moyen continu de la partie contractante comme une moyenne mobile, comme un moyen pour qu'une partie contractante évalue sa propre performance à tout moment.

10.7. Le SSAD DOIT également mesurer la valeur de réponse cible de la moyenne mobile enregistrée à la fin de l'intervalle d'évaluation du temps de réponse cible Seule la valeur de réponse cible sur 3 mois DOIT être utilisée pour déterminer la réussite ou l'échec de l'atteinte des objectifs de réponse décrits ci-dessous. Afin d'éviter toute confusion, le but de fournir à la partie contractante le temps de réponse moyen du SSAD est d'avertir à la partie contractante qu'il peut y avoir un problème avec ses temps de réponse et de lui permettre de remédier à la question de manière coopérative. Les parties contractantes doivent donc avoir accès à tout moment à leur propre valeur de réponse cible actuelle. Si la valeur de réponse cible de la partie contractante dépasse les cinq (5) jours ouvrables, cela NE DOIT PAS entraîner une violation de la politique.

Au lieu de cela, le non-respect d'un objectif de réponse incitera l'ICANN à alerter la partie contractante d'un échec de la réponse cible.

10.8. La partie contractante DOIT répondre à l'avis d'échec de la réponse cible de l'ICANN dans un délai de cinq (5) jours ouvrables.

10.9. La réponse de la partie contractante doit comprendre une justification de la raison pour laquelle la partie contractante n'a pas pu atteindre sa cible de réponse.

10.10. Le non-respect par la partie contractante de la notification de l'ICANN DOIT être considéré comme une violation de la politique ; par conséquent, le non-respect de la notification de conformité entraînera une enquête de conformité de l'ICANN.

ÉTAPE 2 (s'applique uniquement aux requêtes de priorité 3)

10.11. Au cours de l'étape 2, les objectifs de conformité des parties contractantes pour les requêtes de priorité 3 du SSAD seront de dix (10) jours ouvrables.

10.12. Le gestionnaire de la passerelle centrale DOIT mesurer les objectifs de conformité en utilisant un temps de réponse moyen, et non individuellement par

réponse. Le SSAD calculera la cible moyenne de conformité de la partie contractante le dernier jour de l'intervalle d'évaluation de réponse cible.

10.13. Si la valeur de réponse cible de la partie contractante dépasse les dix jours ouvrables, cela entraînera une violation de la politique et, par conséquent, la partie contractante sera soumise à l'application de la conformité.

10.14. Les cibles de réponse et les cibles de conformité DOIVENT être examinées, au minimum, tous les six mois au cours de la première année et par la suite une fois par an (selon le résultat de la première révision).

10.15. Les cibles de réponse pour les demandes de divulgation qui répondent aux critères des réponses entièrement automatisées devraient être développées au cours de l'étape de mise en œuvre, mais elles devraient être inférieures à 60 secondes.

10.16. L'équipe chargée de la révision de la mise en œuvre devrait en outre prendre en compte l'effet des SLA aux cas où des informations supplémentaires seraient demandées à la partie contractante et fournies par le requérant. (Pour de plus amples informations, reportez-vous à la Recommandation 8 - Autorisation de la partie contractante.)

Recommendation #11. Termes et conditions du SSAD

11.1. L'équipe responsable de l'EPDP recommande que les attentes minimales pour les accords et les politiques appropriés, comme les conditions d'utilisation du SSAD, une politique de confidentialité du SSAD, un accord de divulgation et une politique d'utilisation acceptable, soient définies au cours de l'étape de mise en œuvre, à développer et à appliquer par la suite par l'entité responsable du SSAD (par l'organisation ICANN ou un tiers chargé par l'organisation ICANN d'assumer cette fonction d'application). Ces accords et politiques DOIVENT tenir compte de toutes les recommandations de la présente politique. Ces accords et politiques devraient être élaborés et négociés, le cas échéant, par les parties impliquées dans le SSAD, en tenant compte des directives de mise en œuvre ci-dessous.

11.2. Tous les accords nécessaires relatifs au traitement des demandes de données par l'intermédiaire du SSAD doivent inclure des clauses relatives aux transferts transfrontaliers, garantissant un engagement des parties, le cas échéant, d'assurer et de prévoir un niveau adéquat de protection des données.

11.3. Les termes et conditions du SSAD POURRAIENT être mis à jour, le cas échéant, par l'organisation ICANN pour traiter de la loi et des pratiques applicables.

Guide de mise en œuvre :

11.4. Politique en matière de vie privée pour le traitement des données personnelles des utilisateurs du SSAD (requérants du SSAD et parties contractantes) par le SSAD

L'EPDP recommande, au minimum, que la politique en matière de vie privée comporte des principes de protection des données pertinents, notamment :

- Le ou les type/s de données personnelles traitées
- Comment et pourquoi les données personnelles sont traitées, par exemple,
  - vérification de l'identité
  - communication des avis de service
- Durée de la conservation des données personnelles
- Types de tierces parties avec lesquelles les données personnelles sont partagées
- Le cas échéant, les détails de tout transfert de données/exigences internationales s'y rapportant
- Informations sur les droits de la personne concernée et la méthode par laquelle elle peut exercer ces droits
- Notification des modifications apportées à la politique en matière de vie privée
- Exigences de transparence
- Exigences relatives à la sécurité des données
- Mesures de responsabilité (respect de la vie privée dès la conception, par défaut, responsable de la protection des données (DPO) à partir d'une certaine taille, etc.)

11.5. Conditions d'utilisation pour les utilisateurs du SSAD (requérants du SSAD et parties contractantes)

L'EPDP recommande, au minimum, que les conditions d'utilisation DOVIENT aborder :

- L'indemnisation par le requérant des autorités de contrôle (entité responsable de la décision de divulgation) fondée sur les principes suivants :
  - Les requérants sont responsables des dommages ou des coûts liés aux réclamations de tiers résultant (i) de leurs fausses déclarations dans le processus d'accréditation ou de demande ; ou (ii) de l'utilisation abusive des données demandées en violation des conditions d'utilisation applicables ou des lois applicables.
  - Rien dans ces conditions ne limite la responsabilité ou les droits de recouvrement des parties en vertu des lois applicables (c'est à dire, les requérants ne sont pas exclus de la recherche de récupération auprès des contrôleurs lorsque ces droits sont prévus par la loi).
  - Aucune disposition des présentes conditions ne seront interprétées comme créant des obligations d'indemnisation pour les demandeurs

d'autorité publique qui n'ont pas l'autorité légale de conclure de telles clauses d'indemnisation. De plus, rien dans cette clause ne modifie la responsabilité gouvernementale existante comme recours pour les opérateurs du SSAD.

- Exigences relatives à la sécurité des données
- Exigences en matière de journalisation et d'audit
- Capacité à démontrer la conformité
- Interdictions applicables
- Exigences de prévention des abus

11.6. Accords de divulgation pour les requérants du SSAD

L'EPDP recommande, au minimum, que les accords de divulgation DOIVENT aborder les exigences applicables aux requérants une fois que les données leur ont été divulguées :

- Utilisation des données aux fins indiquées dans la requête
- Exigences pour l'utilisation des données à un nouvel usage autre que celui indiqué dans la requête
- Conservation et destruction des données : Les requérants DOIVENT confirmer qu'ils s'occuperont de stocker, protéger et éliminer les données d'enregistrement des gTLD conformément à la loi applicable. Les requérants DOIVENT conserver uniquement les données d'enregistrement gTLD pendant le temps nécessaire pour atteindre l'objectif indiqué dans la requête de divulgation, sauf obligation contraire de conserver ces données pendant une période plus longue en vertu de la loi applicable.
- Utilisation légale des données

11.7. Politique d'utilisation acceptable pour les requérants du SSAD. Le requérant DOIT accepter la Politique d'utilisation acceptable avant que les requêtes de divulgation soient soumises par le biais du SSAD.

Au minimum, la Politique d'utilisation acceptable DOIT inclure les exigences suivantes :

Le requérant :

11.7.1. DOIT uniquement requérir des données de l'ensemble de données RDS actuel (pas des données historiques) ;

11.7.2. DOIT, pour chaque requête de données RDS, fournir des représentations de l'objet correspondant et de la base légale du traitement, qui fera l'objet d'une vérification (consulter la Recommandation 16 d'audit pour plus de détails) ;

11.7.3. POURRAIT requérir des données au SSAD à des fins multiples par demande, pour le même ensemble de données requis ;

11.7.4. Pour chaque objectif déclaré il doit fournir (i) une représentation concernant l'utilisation prévue des données requises et (ii) une représentation selon laquelle le requérant traitera les données uniquement pour le ou les objectif/s indiqué/s. Ces observations feront l'objet d'une vérification (consulter la Recommandation 16 pour de plus amples détails).

Recommendation #12. Obligation de divulgation

12.1. L'équipe responsable de l'EPDP recommande ce qui suit :

Parties contractantes :

12.1.1. DOIVENT divulguer uniquement les données requises par le requérant ;

12.1.2. DOIVENT renvoyer les données actuelles ou un sous-ensemble de celles-ci (pas des données historiques) ;

12.2. Parties contractantes et gestionnaire de la passerelle centrale :

12.2.1. DOIVENT traiter les données conformément à la législation en vigueur ;

12.2.2. Lorsque la loi en vigueur l'exige, ils DOIVENT divulguer au titulaire de nom enregistré (personne concernée), sur demande raisonnable, la confirmation du traitement des données personnelles le concernant en notant, toutefois, que la nature des enquêtes ou procédures juridiques PEUT exiger du SSAD et/ou de l'entité divulgatrice qu'elle conserve la nature ou l'existence de certaines requêtes confidentielles de la personne concernée. Les requêtes confidentielles POURRAIENT être divulguées aux personnes concernées en coopération avec l'entité requérante, et conformément aux droits de la personne concernée en vertu de la loi applicable ;

12.2.3. Lorsque la loi en vigueur l'exige, elles DOIVENT prévoir un mécanisme en vertu duquel la personne concernée puisse exercer son droit d'effacement pour s'opposer au traitement automatisé de ses informations personnelles si ce traitement avait un effet juridique ou tout aussi significatif, ainsi que tout autre droit applicable ;

12.2.4. DOIVENT, sous une forme concise, transparente, intelligible et facilement accessible, en utilisant un langage clair et simple, informer les personnes concernées des types d'entités/de tiers qui pourraient traiter leurs données. Afin d'éviter toute confusion, les parties contractantes DOIVENT fournir l'avis décrit ci-dessus à leurs clients titulaires de noms de domaine, et le SSAD DOIT fournir l'avis décrit ci-dessus aux utilisateurs du SSAD. Pour les parties contractantes, cet avis DOIT contenir des informations sur les destinataires potentiels des données d'enregistrement non publiques, y compris, mais sans s'y limiter, les

destinataires énumérés dans la Recommandation 7 - Objectifs du requérant, suivant ce qui soit juridiquement admissible. Les obligations en matière d'information selon les lois applicables pourraient être également appliquées, mais les informations mentionnées ci-dessus DOIVENT être contenues, au minimum.

Orientations relatives à la mise en œuvre

12.3. Les données actuelles font allusion aux données examinées par la partie contractante lorsque celle-ci détermine si les données devraient être divulguées. Afin de réduire la possibilité de modifications des données pendant la suspension d'une requête de divulgation en suspens, par exemple, si le titulaire de nom de domaine met à jour ses données de contact, les parties contractantes sont encouragées à divulguer les données dès que possible après la décision de divulguer ou non les données. Afin d'éviter toute confusion, les données historiques font référence aux données d'enregistrement en place avant la présentation de la requête de divulgation, pas aux données d'enregistrement qui pourraient avoir changé à la suite de mises à jour effectuées par le titulaire de nom de domaine entre le moment où la requête de divulgation est examinée et la décision de divulguer les données d'enregistrement.

12.4. La nature des enquêtes ou procédures judiciaires ne se limite pas aux enquêtes criminelles ou à d'autres enquêtes (par exemple, de nombreuses enquêtes civiles exigent le respect de la vie privée).

Recommendation #13. Politique applicable aux requêtes

13.1. La recommandation de l'équipe responsable de l'EPDP indique que le gestionnaire de la passerelle centrale :

13.1.1. DOIT surveiller le système et prendre les mesures appropriées,[34] telles que la révocation ou la limitation de l'accès, pour se protéger contre l'utilisation malveillante ou abusive du système ;

13.1.2. POURRAIT prendre des mesures pour limiter le nombre de requêtes soumises par le même requérant s'il était démontré que les requêtes sont de nature abusive ;

L'utilisation « abusive » du SSAD POURRAIT comprendre (sans s'y limiter) la détection d'un ou plusieurs des comportements/pratiques suivants :

13.1.2.1. L'envoi automatisé de gros volumes de requêtes mal formées ou incomplètes.

[34] L'équipe responsable de l'EPDP s'attend à ce que des « mesures appropriées » soient définies au cours de l'étape de mise en œuvre.

13.1.2.2. Des requêtes en double automatisées à volume élevé[35] qui soient frivoles, malveillantes ou vexatoires.

13.1.2.3. L'utilisation de données d'identification fausses, volées ou contrefaites pour accéder au système.

13.1.2.4. Le stockage/report et envoi de requêtes à volume élevé entraînant l'échec des performances prévues au SLA du SSAD ou d'autres parties. Lorsqu'il s'agit d'enquêter sur des abus fondés sur ce comportement spécifique, le concept de proportionnalité doit être considéré.

13.1.3. Comme pour les autres violations de la politique d'accès, un comportement abusif peut en fin de compte entraîner la suspension ou la résiliation de l'accès au SSAD. Au cas où le responsable de la passerelle centrale prendrait une décision fondée sur un abus pour limiter le nombre de requêtes d'un requérant, le requérant POURRAIT demander la réparation[36] via l'organisation ICANN s'il estimait que la détermination est injustifiée. Afin d'éviter toute confusion, si le SSAD reçoit un grand nombre de requêtes du même requérant, le volume à lui seul ne doit pas entraîner une détermination de facto de l'abus du système.

13.1.4. DOIT répondre uniquement aux requêtes associées à un nom de domaine spécifique pour lequel la divulgation des données d'enregistrement non publiques est requise et DOIT examiner[37] chaque requête individuellement et pas en masse, peu importe si la considération est effectuée automatiquement ou à travers un examen approfondi.

13.2. La recommandation de l'équipe responsable de l'EPDP indique que les parties contractantes :

13.2.1. NE DOIVENT PAS rejeter les requêtes de divulgation de la part du SSAD en raison d'un comportement abusif qui n'ait pas été jugé abusif par le gestionnaire de la passerelle centrale conformément aux points a) et b) ci-dessus. Toutefois, les parties contractantes doivent également disposer de certains moyens pour signaler ce comportement au CGM/SSAD. Le responsable de la passerelle centrale DOIT fournir un mécanisme permettant aux parties contractantes de signaler les

[35] L'équipe responsable de l'EPDP s'attend à ce que le « volume élevé » soit défini au cours de l'étape de mise en œuvre.

[36] Pour plus de clarté, la réparation serait sous forme de réexamen par le gestionnaire de la passerelle centrale, pour lequel le requérant peut fournir de nouvelles informations, mais n'étant pas tenu de le faire.

[37] Il est prévu que cet examen soit automatisé.

requérants/requêtes abusives perçues et de fournir une décision concernant le requérant/la requête dans les délais autorisés pour que la partie contractante puisse donner une réponse. Ou encore, la partie contractante sera autorisée à retarder la réponse jusqu'à ce que le responsable de la passerelle centrale ait examiné la déclaration d'abus et ait pris une décision.

13.3. L'équipe responsable de l'EPDP recommande ce qui suit :

13.3.1. Le gestionnaire de la passerelle centrale DOIT prendre en charge les requêtes saisies sur des noms de domaine complètement qualifiés (sans caractères génériques).

13.3.2. Le gestionnaire de la passerelle centrale DOIT prendre en charge la capacité d'un requérant à soumettre plusieurs noms de domaine en une seule requête.[38]

13.3.3. Pour les requêtes de divulgation n'étant pas soumises au traitement automatisé de la décision de divulgation, le gestionnaire de la passerelle centrale DOIT acheminer chaque domaine individuellement à la partie contractante responsable de la décision de divulgation (il peut être nécessaire que le SSAD divise une requête en plusieurs transactions).

13.3.4. Nonobstant les recommandations relatives à la gestion des comportements abusifs, le gestionnaire de la passerelle centrale et les parties contractantes DOIVENT avoir la capacité de traiter un nombre raisonnable de requêtes conformément aux SLA établis.

13.3.5. Le gestionnaire de la passerelle centrale DOIT prendre en charge uniquement les requêtes de données actuelles (aucune donnée sur l'historique de l'enregistrement du nom de domaine).

13.3.6. La SSAD DOIT être en mesure de sauvegarder l'historique des différentes requêtes de divulgation, afin de conserver la traçabilité des échanges entre les requérants du SSAD et les parties contractantes via le SSAD. Des mesures de protection appropriées doivent être mises en place pour protéger ces informations. Un accès approprié à ces statistiques d'activité pertinentes devrait être fourni aux parties contractantes, si cela était jugé nécessaire, pour s'assurer que toutes les informations pertinentes relatives aux requêtes de divulgation soient disponibles pour examen dans ces décisions de divulgation.

Consulter également les exigences de la politique d'utilisation acceptable dans la Recommandation 11 – Conditions générales.

Orientations relatives à la mise en œuvre

[38] L'équipe responsable de l'EPDP s'attend à ce que la mise en œuvre détermine raisonnablement combien de requêtes peuvent être soumises à la fois, conformément à la politique de requête.

13.4. Un comportement abusif peut en fin de compte entraîner la suspension ou la cessation de l'accès au SSAD ; toutefois, un régime de pénalité progressive devrait être envisagé dans la mise en œuvre. Il peut toutefois y avoir certains cas d'abus flagrants, comme la contrefaçon ou le vol de titres de compétence, où la résiliation serait immédiate.

13.5. Une demande SSAD doit être reçue pour chaque enregistrement de nom de domaine pour lequel il est requis que l'enregistrement non public soit divulgué, mais il doit être possible pour les requérants de soumettre plusieurs requêtes en même temps, par exemple, en saisissant plusieurs enregistrements de noms de domaine dans le même formulaire de requêtes, à condition que les mêmes informations de requêtes soient appliquées.

13.6. En ce qui concerne « l'accès approprié à ces statistiques d'activité pertinentes devrait être fourni aux parties contractantes, si cela était jugé SSAD ; nécessaire » en 13.3, cette information devrait être limitée à l'activité propre d'une partie contractante.

Recommendation #14. Viabilité financière

14.1. L'équipe responsable de l'EPDP recommande que, en tenant compte des coûts et de la viabilité financière du SSAD, il soit nécessaire de faire la distinction entre le développement et l'opérationnalisation du système et le fonctionnement ultérieur du système.

14.2. L'objectif est que le SSAD puisse être financièrement auto-suffisant et n'entraîne pas de frais supplémentaires pour les titulaires de noms de domaine. Les personnes concernées NE DOIVENT PAS supporter les coûts liés à la divulgation de données à des tiers ; les requérants des données du SSAD doivent principalement assumer les coûts associés à l'entretien ce système. En outre, les personnes concernées ne DOIVENT PAS endosser les frais du traitement des requêtes de divulgation des données qui ont été refusées par les parties contractantes suite à l'évaluation de la requête soumise par les utilisateurs du SSAD. L'ICANN POURRAIT contribuer à la prise en charge (partielle) des coûts d'entretien de la passerelle centrale. Pour plus de clarté, l'équipe responsable de l'EPDP considère que les titulaires de noms de domaine sont la source première d'une grande partie des revenus de l'ICANN. Ce revenu ne viole pas en soi la restriction selon laquelle « les personnes concernées NE DOIVENT PAS assumer les coûts de la divulgation de données à des tiers ». La passerelle centrale ne DOIT PAS facturer aux personnes concernées des frais distincts pour la divulgation ou la requête de données à des tiers. Toutefois, l'équipe responsable de l'EPDP note que les titulaires de noms enregistrés assumeront toujours indirectement tous les coûts engagés par les bureaux d'enregistrement et les opérateurs de registre. L'équipe responsable de l'EPDP comprend également que le RAA interdit à l'ICANN de limiter ce que les bureaux d'enregistrement peuvent facturer. Le point 3.7.12 du RAA établit que

: « Aucune disposition du présent contrat ne prescrit ni limite le montant que le bureau d'enregistrement peut facturer aux titulaires des noms enregistrés pour l'enregistrement des noms enregistrés ».

14.3. Les utilisateurs éventuels du SSAD, selon ce qui est déterminé en fonction de la mise en œuvre du processus d'accréditation et des fournisseurs d'identité à utiliser, devraient être consultés sur la fixation des frais d'utilisation du SSAD. En particulier, les requérants potentiels du SSAD qui ne font pas partie de la communauté de l'ICANN doivent avoir la possibilité de commenter et d'interagir avec l'IRT. Cette contribution devrait aider à éclairer les délibérations de l'IRT sur ce sujet.

14.4. Le SSAD NE DEVRAIT PAS être considéré comme une plateforme génératrice de profits pour l'ICANN ou les parties contractantes. Le financement du SSAD devrait être suffisant pour couvrir les coûts, y compris pour les sous-traitants à la juste valeur marchande et pour établir un fonds de risque juridique.[39] Il est essentiel de s'assurer que tous les paiements dans le SSAD soient liés aux coûts opérationnels et ne soient pas simplement un échange de fonds pour des données d'enregistrement non publiques.

14.5. En ce qui concerne le cadre d'accréditation :

- 14.5.1. Les demandeurs d'accréditation DOIVENT payer des frais non remboursables à déterminer qui soient proportionnels au coût de validation d'une demande, sauf dans certaines circonstances où ces frais pourraient être annulés ou nuls pour certains types ou catégories de demandeurs qui DEVRAIENT être définis plus en détail pendant l'étape de mise en œuvre.
- 14.5.2. Les demandeurs rejetés POURRAIENT présenter une nouvelle demande, mais la ou les nouvelles demandes POURRAIENT être soumises aux frais de demande.
- 14.5.3. Les frais doivent être établis par l'autorité d'accréditation. Si l'autorité d'accréditation externalise la fonction de fournisseur d'identité, celui-ci PEUT établir ses propres frais après consultation avec l'autorité d'accréditation.
- 14.5.4. Les utilisateurs et les organisations accrédités DOIVENT renouveler périodiquement leur accréditation.

Orientations relatives à la mise en œuvre

14.6. L'équipe responsable de l'EPDP s'attend à ce que les coûts de développement, de déploiement et d'opérationnalisation du système, similaires à la mise en œuvre

[39] Étant donné le risque potentiel d'incertitude juridique et le risque juridique et opérationnel accru pour toutes les parties incluses dans la fourniture du SSAD, la création d'un fonds de risque juridique signifie la création d'un plan d'urgence juridique approprié, y compris, mais sans s'y limiter, une couverture d'assurance appropriée, et toute autre mesure appropriée pouvant être jugée suffisante pour couvrir les éventuelles amendes réglementaires ou les frais juridiques connexes.

d'autres recommandations politiques adoptées, soient initialement supportés par l'organisation ICANN,[40] les parties contractantes et d'autres parties qui pourraient être impliquées.[41] Dans le cadre de l'opérationnalisation du SSAD, l'organisation ICANN devrait envisager de s'appuyer sur les mécanismes existants ou d'utiliser un processus d'appel à propositions (RFP) pour réduire les coûts plutôt que de construire le SSAD et ses composantes à partir de zéro. L'équipe responsable de l'EPDP s'attend à ce que le SSAD entraîne en fin de compte des coûts égaux ou inférieurs pour les parties contractantes par rapport à la réception manuelle et à la révision des requêtes comme mesure de faisabilité commerciale et technique.

14.7. Le fonctionnement ultérieur du système devrait se faire sur la base du recouvrement des coûts, selon lequel les coûts historiques[42] peuvent être pris en compte. Par exemple, les coûts associés à l'accréditation seraient assumés par ceux qui cherchent à obtenir l'accréditation. De même, une partie des coûts de fonctionnement du SSAD DEVRAIT être compensée par l'imposition de frais aux utilisateurs du SSAD.

14.8. Lors de la mise en œuvre et de l'exploitation du SSAD, il convient d'éviter une charge disproportionnée sur les petits opérateurs.

14.9. L'équipe responsable de l'EPDP reconnaît que les frais associés à l'utilisation du SSAD peuvent différer pour les utilisateurs en fonction du volume de requêtes ou du type d'utilisateur, entre autres facteurs potentiels. L'équipe responsable de l'EPDP reconnaît également que les gouvernements peuvent être soumis à certaines restrictions de paiement qui devraient être prises en compte dans le cadre de la mise en œuvre.

14.10. La structure des frais ainsi que la période de renouvellement doivent être déterminées au cours de l'étape de mise en œuvre, conformément aux principes énoncés ci-dessus. L'équipe responsable de l'EPDP reconnaît qu'il n'est pas possible de fixer les frais exacts tant que les coûts réels ne soient pas connus. L'équipe responsable de l'EPDP reconnaît également que la structure des frais du SSAD peut devoir être examinée au fil du temps.

Recommendation #15. Journalisation

15.1. La recommandation de l'équipe responsable de l'EPDP indique que les procédures de journalisation appropriées DOIVENT être mises en place pour faciliter les

[40] Consulter également les informations fournies par l'organisation ICANN sur la demande de l'équipe responsable de l'EPDP par rapport à l'estimation des coûts pour un système d'accès et de divulgation normalisé proposé (consulter https://community.icann.org/x/GIIEC)

[41] Pour plus de clarté, l'organisation ICANN supportera ses propres coûts pour le développement du système. Les parties contractantes seront responsables de leurs propres coûts.

[42] Les coûts historiques se réfèrent aux coûts de développement, de déploiement et d'opérationnalisation du système.

procédures d'audit décrites dans les présentes recommandations. Ces exigences de journalisation couvrent les éléments suivants :

- Autorité d'accréditation
- Gestionnaire de la passerelle centrale
- Fournisseur d'identité
- Parties contractantes
- Activité des utilisateurs accrédités, comme les tentatives de connexion, les requêtes
- Quelles sont les demandes et les décisions de divulgation prises

15.2. L'équipe responsable de l'EPDP recommande ce qui suit :

15.2.1. Le gestionnaire de la passerelle centrale DOIT établir des journaux de toutes les activités de toutes les entités qui interagissent avec le gestionnaire de la passerelle centrale (pour de plus amples détails, consulter ci-dessous).

15.2.2. Les journaux DOIVENT inclure un enregistrement de toutes les requêtes et de tous les éléments nécessaires à l'audit des décisions prises dans le contexte du SSAD.

15.2.3. Les journaux DOIVENT être conservés pendant une période suffisante pour l'audit et la résolution des plaintes, en tenant compte des limites légales liées aux plaintes déposées contre le contrôleur.

15.2.4. Les journaux NE DOIVENT contenir aucune information personnelle. Si des renseignements qui contiennent des renseignements personnels sont consignés, des mesures de protection appropriées doivent être mises en place. Les journaux PEUVENT être utilisés pour les rapports de transparence, qui peuvent être rendus publics. (Consulter aussi la Recommandation 17 sur les exigences en matière de rapports). Les données consignées contenant des informations personnelles DOIVENT rester confidentielles.

15.2.5. Les journaux DOIVENT être conservés dans un format couramment utilisé,[43] lisible par machine, accompagné d'une description intelligible de toutes les variables.

15.2.6. Les données consignées pertinentes DOIVENT être divulguées, lorsque la loi l'autorise, dans les circonstances suivantes :

- En cas de réclamation pour abus, les journaux peuvent faire l'objet d'un examen par une autorité d'accréditation ou un fournisseur de règlement de litiges.
- Les journaux doivent être mis à la disposition de l'ICANN et de l'organe d'audit.

[43] Pour plus de clarté, « couramment » signifie un format qui est largement utilisé, pas un format uniforme pour tous.

- Lorsque le mandat est exigé à la suite d'une procédure légale, y compris les autorités de contrôle et d'application de la loi pertinentes, le cas échéant.

15.2.7. Les données consignées pertinentes PEUVENT être divulguées pour :

- Le fonctionnement technique général afin de garantir le bon fonctionnement du système.

15.2.8. Les journaux pertinents devraient être utilisés comme source pour mettre à disposition toutes les données pertinentes. Ces données devraient permettre aux requérants et aux parties contractantes de consulter leurs propres statistiques.

15.3. Au minimum, les incidents suivants DOIVENT être consignés :

- Journalisation liée au fournisseur d'identité[44]
- Journalisation liée à l'autorité d'accréditation
  - Détails des demandes d'accréditation entrantes
  - Résultats du traitement des demandes d'accréditation, par exemple la délivrance des justificatifs d'identité ou les motifs de refus
  - Détails des demandes de révocation
  - Indication lorsque les informations d'identification et les assertions signées ont été validées.
  - Numéro de référence unique
- Journalisation liée au gestionnaire de la passerelle centrale
  - Informations liées aux contenus de la requête elle-même.
  - Résultats du traitement de la requête, y compris les changements d'état (par exemple, reçu, en attente, en cours de traitement, refusé, approuvé, approuvé avec modifications)
  - Tarifs :
    - divulgation et non-divulgation ;
    - utilisation de chaque motif de refus de non-divulgation ;
    - divergence entre les décisions de communication et de non-divulgation d'une partie contractante et les recommandations de la passerelle centrale.

Journalisation relative aux parties contractantes

- Détails de la réponse à la requête, par exemple, motif du refus, avis d'approbation et champs de données libérés. Les décisions de divulgation, y compris un motif de refus, doivent être stockées.

Recommendation #16. Audits

16.1. La recommandation de l'équipe responsable de l'EPDP indique que les processus et procédures de vérification appropriés DOIVENT être mis en place afin

44 Plus détaillé dans l'étape de mise en œuvre.

d'assurer une surveillance et une conformité appropriées aux exigences énoncées dans les présentes recommandations.

16.2. Dans le cadre de toute vérification, l'auditeur DOIT être assujetti à des obligations raisonnables de confidentialité en ce qui concerne les processus propriétaires et les renseignements personnels divulgués au cours de la vérification.

Plus spécifiquement :

Audits de l'autorité d'accréditation

16.3. Si l'ICANN externalise la fonction d'autorité d'accréditation à un tiers qualifié, l'autorité d'accréditation DOIT faire l'objet d'un audit périodique afin de garantir la conformité aux exigences de la politique telles que définies dans la recommandation d'accréditation. Si l'autorité d'accréditation était jugée non conforme à la politique et aux exigences d'accréditation, elle aura la possibilité de remédier à la violation, mais en cas de défaillance répétée, une nouvelle autorité d'accréditation doit être identifiée ou créée. L'organisation ICANN en tant qu'autorité d'accréditation n'est pas tenue d'auditer les entités gouvernementales dont les exigences d'accréditation et d'audit sont définies dans la Recommandation 2.

16.4. Tout audit à l'autorité d'accréditation DOIT être adapté afin d'évaluer la conformité, et l'auditeur DOIT prévenir d'un tel contrôle avec un préavis raisonnable, en indiquant avec suffisamment de détails les catégories de documents, données et autres informations requises.

16.5. Dans le cadre de ces audits, l'autorité d'accréditation DOIT fournir à l'auditeur, en temps opportun, tous les documents, données et autres renseignements pertinents nécessaires pour démontrer sa conformité à la politique d'accréditation.

16.6. Si l'ICANN sert d'autorité d'accréditation, les mécanismes de responsabilité existants sont censés traiter toute violation de la politique d'accréditation, en notant que dans un cas aussi extrême, les références émises au moment de la violation seront examinées. Les modalités de cet examen DEVRAIENT être établies au cours de l'étape de mise en œuvre.

Audits des fournisseurs d'identité

16.7. Les fournisseurs d'identité DOIVENT être vérifiés périodiquement pour s'assurer de la conformité aux exigences de la politique telles que définies dans la recommandation d'accréditation. Si le fournisseur d'identité était jugé non conforme à la politique et aux exigences d'accréditation, il aurait la possibilité

de remédier à la violation, mais en cas de défaillance répétée, une nouvelle autorité d'accréditation devrait être identifiée ou créée.

16.8. Tout audit au fournisseur d'identité DOIT être adapté afin d'évaluer la conformité, et l'auditeur DOIT prévenir d'un tel audit avec un préavis raisonnable, en indiquant de manière suffisamment détaillée les catégories de documents, données et autres informations requises.

16.9. Dans le cadre de ces audits, le fournisseur d'identité DOIT fournir à l'auditeur, en temps opportun, tous les documents, données et autres informations utiles pour démontrer sa conformité à la politique d'accréditation.

Audits des entités/personnes accréditées

16.10. Des mécanismes appropriés DOIVENT être créés au cours de l'étape de mise en œuvre afin d'assurer la conformité des entités accréditées et des individus aux exigences de la politique telles que définies dans les Recommandations d'accréditation 1 et 2. Il peut s'agir, par exemple, de vérifications déclenchées par des plaintes vérifiées, des audits aléatoires ou des audits en réponse à une auto-certification ou à une auto-évaluation. Si l'entité ou la personne accréditée est jugée avoir violé la politique et les exigences d'accréditation, elle aura la possibilité de remédier à la violation. Toutefois, en cas de non-conformité répétée ou d'échec de l'audit, le problème devra être renvoyé à l'autorité d'accréditation et/ou au fournisseur d'identité, le cas échéant, pour décider des actions.

16.11. Tout audit aux entités/personnes accréditées DOIT être adapté afin d'évaluer la conformité, et l'auditeur DOIT prévenir d'un tel audit avec un préavis raisonnable, en indiquant avec suffisamment de détails les catégories de documents, données et autres informations requises.

16.12. Dans le cadre de ces audits, l'entité ou la personne accréditée DOIT, en temps opportun, fournir à l'auditeur tous les documents, données et autres renseignements pertinents nécessaires pour démontrer sa conformité à la politique d'accréditation.

Recommendation #17. Exigences concernant les rapports

17.1. L'équipe responsable de l'EPDP recommande que l'organisation ICANN DOIT établir des rapports publics réguliers sur l'utilisation et le fonctionnement du SSAD. Afin d'éviter toute confusion, cette recommandation n'a pas pour but d'empêcher l'organisation ICANN d'effectuer des rapports non publics supplémentaires aux utilisateurs du SSAD.

17.2. Au plus tôt 3 mois et au plus tard 9 mois après l'opérationnalisation du SSAD, l'organisation ICANN DOIT publier un rapport ou un tableau de bord du SSAD, et continuer à le faire tous les trois mois. Ledit rapport inclura au minimum :

- Le nombre de requêtes de divulgation automatisées ;
- Les temps de réponse moyens aux requêtes de divulgation, classés par niveau de priorité ;
- Le nombre de requêtes classées suivant les objectifs / justifications des tierces parties (tel qu'indiqué dans la Recommandation 4) ;
- Le nombre de requêtes de divulgation approuvées et refusées ;
- Le nombre de requêtes de divulgation automatisées ;
- Le nombre de requêtes traitées manuellement ;
- Les informations sur la viabilité financière du SSAD ;
- La nouvelle directive du CEPD ou nouvelle jurisprudence d'actualité (le cas échéant) ;
- Les difficultés techniques ou du système ;
- Les améliorations opérationnelles et DOIT être du système.

Guide de mise en œuvre :

17.3. L'équipe responsable de l'EPDP recommande de prendre davantage en considération les points suivants au cours de la mise en œuvre :

- La fréquence des rapports publics – les rapports publics trimestriels seraient considérés raisonnables ;
- Les données à signaler, qui doivent inclure des informations telles que : a) le nombre de requêtes de divulgation ; b) les requêtes de divulgation par catégorie de requérants ; c) les requêtes de divulgation par requérant (pour les entités juridiques) ; les requêtes de divulgation accordées / refusées et ; les délais de réponse. Veuillez noter que cette liste n'est pas exhaustive.
- Mécanisme de rapport au public – envisager la possibilité d'un tableau de bord accessible au public au lieu ou en plus des rapports publiés ;
- Le besoin du respect de la vie privée dans certains cas, tels que les informations sur les personnes physiques et les demandes de l'application de la loi. Les données agrégées ou la pseudonymisation pourraient être considérées pour répondre à des préoccupations possibles en matière de respect de la vie privée.

Recommendation #18. Révision de la mise en œuvre des recommandations de politiques concernant le SSAD à l'aide d'un Comité permanent de la GNSO

18.1. La révision de l'équipe responsable de l'EPDP indique que le conseil de la GNSO DOIT établir un comité permanent pour évaluer les problèmes opérationnels du

SSAD qui émergent suite à l'adoption des politiques de consensus de l'ICANN et/ou à leur mise en œuvre. Le Comité permanent de la GNSO a pour but d'examiner les données produites à la suite des opérations du SSAD et de fournir au conseil de la GNSO des recommandations sur la meilleure façon d'apporter des changements opérationnels au SSAD, qui sont strictement des mesures de mise en œuvre, en plus des recommandations fondées sur l'examen de l'impact des politiques de consensus existantes sur les opérations du SSAD.

18.2. L'équipe responsable de l'EPDP recommande également que le conseil de la GNSO utilise les principes suivants comme base pour que le Comité permanent de la GNSO puisse s'acquitter de sa mission, qui doit être reflétée dans sa charte :

18.2.1 Composition : La composition du Comité permanent de la GNSO sera représentative des comités consultatifs de l'ICANN, des groupes de parties prenantes et des unités constitutives de la GNSO représentés dans l'équipe responsable de l'EPDP actuel sur la spécification temporaire relative aux données d'enregistrement des gTLD. Cette composition comprendra au moins un membre du GAC, un de l'ALAC, un du SSAC, un du RySG, un du RrSG, un du NCSG, un de l'IPC, un de la BC et un de l'ISPCP, ainsi qu'au moins un membre suppléant de chaque groupe. Il est à noter que le nombre de membres par groupe ne devrait pas avoir d'incidence sur le processus de désignation par consensus puisque les postes devraient être pris en compte par groupe et pas au niveau individuel des membres. Le conseil de la GNSO peut également envisager d'inviter les agents de liaison de l'organisation ICANN en tant que membres du Comité permanent de la GNSO.

18.2.2. Portée : Une charte pour le Comité permanent de la GNSO doit être élaborée par le conseil de la GNSO en collaboration avec les comités consultatifs, par exemple le GAC, le SSAC et l'ALAC. La charte doit permettre au Comité d'aborder toutes les questions opérationnelles concernant le SSAD. Cela peut inclure, sans s'y limiter, des sujets tels que les conventions de service (SLA), la centralisation/décentralisation, l'automatisation, les objectifs de tiers, la viabilité financière et les améliorations opérationnelles et du système. Le seuil d'acceptation d'une question incluse dans l'ordre du jour du Comité permanent de la GNSO sera suffisamment bas pour permettre que les intérêts de chacun aux opérations du SSAD des groupes concernés soient sérieusement examinés L'identification des questions que le Comité peut traiter est déterminée à l'aide des deux méthodes suivantes :

i. Tout sujet de politique ou de mise en œuvre concernant les opérations du SSAD peut être soulevé par un membre du Comité permanent de la GNSO et est inscrit à l'ordre du jour de travail du

Comité s'il est appuyé par au moins un autre membre du Comité du « groupe ».

ii. En outre, le conseil de la GNSO peut identifier les problèmes opérationnels du SSAD. Le conseil de la GNSO peut choisir de charger le Comité permanent de la GNSO d'évaluer les questions qu'il identifie afin que le Comité fournisse au conseil des recommandations consensuelles des parties prenantes concernées sur la meilleure façon de les aborder.

Les recommandations concernant les directives de mise en œuvre seront envoyées au conseil de la GNSO pour examen et adoption, après quoi elles seront envoyées à l'organisation ICANN pour d'autres travaux de mise en œuvre. Les recommandations qui nécessitent des modifications des politiques de consensus existantes de l'ICANN doivent être enregistrées et mises à jour, afin d'être utilisées dans l'étape de définition de la portée des questions de l'élaboration et/ou de la révision des politiques futures.

18.2.3. Consensus requis : Niveau de consensus pour les recommandations du Comité permanent de la GNSO : Les recommandations sur les opérations et les politiques du SSAD élaborées par le Comité permanent doivent parvenir à un consensus des membres du Comité afin d'être envoyées sous forme de recommandations officielles au conseil de la GNSO. Pour que les recommandations obtiennent une désignation par consensus, le soutien des parties contractantes sera nécessaire. Aux fins de l'évaluation du niveau de consensus, les membres sont tenus de représenter la position officielle de leur SG/C ou SO/AC, et non les points de vue ou les positions individuels. Aux fins de la détermination du niveau de consensus, chacun des neuf groupes comprenant un consensus doit avoir un poids égal sous réserve de l'obligation pour les parties contractantes de soutenir des recommandations spécifiques.

18.2.4. Dissolution du Comité permanent de la GNSO : Le Comité permanent peut recommander au conseil de la GNSO de dissoudre le Comité lui-même, en cas de besoin. Pour que le Comité permanent recommande au conseil de la GNSO de le dissoudre, un vote affirmatif de la majorité simple des groupes concernés est nécessaire. Cette recommandation devra par la suite être adoptée par le conseil de la GNSO.

3.6 Recommandations de priorité 2 de l'équipe responsable de l'EPDP

Recommendation #19. Affichage de l'information des sociétés affiliées et/ou des fournisseurs des services d'anonymisation et d'enregistrement fiduciaire accrédités

19.1. Dans le cas d'un enregistrement de nom de domaine où un affilié et/ou un service d'anonymisation et d'enregistrement fiduciaire accrédité soit utilisé, par exemple, lorsque les données associées à une personne physique sont masquées, le bureau d'enregistrement (et l'opérateur de registre, le cas échéant) DOIT inclure les données RDDS complètes du service d'anonymisation ou d'enregistrement fiduciaire accrédité dans sa réponse à une requête RDDS. Les données RDDS complètes d'anonymisation et d'enregistrement fiduciaire peuvent également inclure un e-mail pseudonymisé.

Notes sur la mise en œuvre :
19.2. Une fois que l'organisation ICANN aura mis en œuvre un programme d'accréditation des services d'anonymisation et d'enregistrement fiduciaire et que cette Recommandation 19 sera en vigueur, cette dernière remplacera ou annulera autrement la Recommandation 14 de l'étape 1 de l'EPDP.
19.3. L'objectif de cette recommandation est de fournir des instructions claires aux bureaux d'enregistrement (et aux opérateurs de registre, le cas échéant) selon lesquelles, lorsqu'un enregistrement de domaine est effectué par l'intermédiaire d'un fournisseur de services d'anonymisation et d'enregistrement fiduciaire affilié et/ou accrédité, ces données NE DOIVENT PAS être expurgées. Le groupe de travail estime que les données d'enregistrement de domaine NE DOIVENT PAS être à la fois expurgées et soumises à l'enregistrement fiduciaire/anonymisation.

Recommendation #20. Expurgation du champ « ville »

L'équipe responsable de l'EPDP recommande que la Recommandation 11 de l'étape 1 de l'EPDP soit mise à jour pour indiquer que l'expurgation POURRAIT être appliquée au champ « ville » en référence aux informations de contact du titulaire de nom de domaine, au lieu de DOIT.

Recommendation #21. Conservation de données

L'équipe responsable de l'EPDP confirme sa recommandation de l'étape 1 selon laquelle les bureaux d'enregistrement DOIVENT conserver uniquement les éléments de données jugés nécessaires aux fins de la politique de règlement de litiges relatifs au transfert (TDRP), pour une période de quinze mois après la durée de l'enregistrement, plus trois mois pour mettre en œuvre la suppression, soit 18 mois. Cette conservation est fondée sur une disposition de la politique énoncée dans la TDRP, qui prévoit que les plaintes présentées aux termes de la politique ne peuvent être déposées que pendant la période des 12 mois suivant la violation alléguée (FN : consulter l'article 2.2 de la TDRP) de la politique de transfert (FN : consulter l'article 1.15 de la TDRP). Pour plus de

clarté, cela n'empêche pas les requérants, y compris le service de conformité de l'ICANN, de requérir la divulgation de ces éléments de données conservés à des fins autres que la TDRP, mais dont la divulgation sera soumise aux lois pertinentes sur la protection des données, par exemple, l'existence d'une base légale pour la divulgation. Afin d'éviter toute confusion, cette période de conservation ne limite pas la capacité des opérateurs de registre et des bureaux d'enregistrement de conserver des éléments de données pendant de longues périodes.

Guide de mise en œuvre :
Afin d'éviter toute confusion, les bureaux d'enregistrement sont tenus de conserver les données pendant 15 mois après la durée de l'enregistrement et POURRAIENT supprimer ces données après une période de 15 mois.

Pour plus de clarté, cela n'empêche pas l'identification de périodes de rétention supplémentaires aux fins indiquées par les autorités de contrôle, telles qu'identifiées et établies par les autorités de contrôle, à des fins autres que la TDRP ; cela n'exclut pas la divulgation potentielle de telles données conservées à une partie quelconque, sous réserve des lois de protection des données pertinentes.

Recommendation #22. Finalité 2
L'équipe responsable de l'EPDP recommande que la finalité suivante s'ajoute à celles de l'étape 1, qui constituent la base de la nouvelle politique de l'ICANN :

- Contribuer au maintien de la sécurité, la stabilité et la résilience du système des noms de domaine, conformément à la mission de l'ICANN.

3.7 Conclusions de l'équipe responsable de l'EPDP sur la priorité 2

Conclusion – Finalité du bureau du directeur de la technologie (OCTO)
Après avoir examiné cette contribution, la plupart des membres de l'équipe responsable de l'EPDP ont convenu qu'à ce stade, il n'est pas nécessaire de proposer une ou plusieurs finalités supplémentaires pour faciliter la réalisation de la mission du bureau du directeur de la technologie (OCTO) de l'ICANN. La raison de cet accord est que la nouvelle finalité 2 de l'ICANN couvre suffisamment le travail de L'OCTO, ainsi que le travail d'autres équipes organisationnelles de l'ICANN telles que l'équipe chargée de la conformité contractuelle et d'autres. La plupart ont également convenu que la décision de l'équipe responsable de l'EPDP de ne pas proposer une ou plusieurs finalités supplémentaires n'empêcherait pas l'organisation et/ou la communauté de l'ICANN d'identifier des finalités supplémentaires pour soutenir des activités futures non identifiées qui pourraient nécessiter l'accès à des données d'enregistrement non publiques.

Conclusion – Exactitude et système de signalement de problèmes liés à l'exactitude du WHOIS

Conformément aux instructions du conseil de la GNSO, l’équipe responsable de l’EPDP n’examinera pas ce sujet plus en détail ; plutôt, le conseil de la GNSO devrait former une équipe de détermination de la portée afin d’explorer davantage les problèmes liés à l’exactitude et l’ARS devrait aider à prendre une décision sur les prochaines étapes appropriées pour traiter les problèmes potentiels identifiés.

4 Prochaines étapes

4.1 Prochaines étapes

Ce rapport final sera présenté au conseil de la GNSO à des fins d'examen et d'approbation. Si le rapport final était adopté par le conseil de la GNSO, il serait ensuite transmis au Conseil d'administration de l'ICANN pour examen et, éventuellement, pour son approbation en tant que politique de consensus de l'ICANN.

Glossaire

1. Comité consultatif
Un comité consultatif est un organe consultatif formel constitué de représentants de la communauté Internet et chargé de prodiguer des conseils à l'ICANN sur un sujet ou un domaine réglementaire spécifique. Un certain nombre de ces comités sont prévus dans les statuts de l'ICANN et d'autres peuvent être créés selon les besoins. Les comités consultatifs ne possèdent aucune autorité légale pour agir au nom de l'ICANN. Ils présentent leurs conclusions et formulent des recommandations au Conseil d'administration de l'ICANN.

2. ALAC - Comité consultatif At-Large
Le Comité consultatif At-large (ALAC) de l'ICANN a pour mission d'étudier et de proposer des recommandations sur les activités de l'ICANN qui se rapportent aux intérêts des utilisateurs individuels d'Internet (« At-Large » faisant référence à la communauté « au sens large »). En tant qu'organisation privée à but non lucratif, responsable de la gestion technique du système des noms de domaine et d'adresses de l'Internet, l'ICANN s'appuiera sur ALAC et son infrastructure de soutien pour assurer la participation et la représentation d'un large éventail d'intérêts des utilisateurs individuels.

3. Unité constitutive des représentants des utilisateurs commerciaux (BC)
L'Unité constitutive des utilisateurs commerciaux représente les utilisateurs commerciaux de l'Internet. Elle est l'une des unités constitutives appartenant au Groupe des représentants des entités commerciales (CSG) visé au chapitre 11.5 des statuts constitutifs de l'ICANN. La BC est l'une de parties prenantes et unités constitutives de l'organisation de soutien aux extensions génériques (GNSO) chargée de conseiller le Conseil d'administration de l'ICANN sur les questions de politique relatives à la gestion du système des noms de domaine.

4. ccNSO - Organisation de soutien aux extensions géographiques
La ccNSO est l'organisation de soutien chargée d'élaborer et de recommander au Conseil d'administration de l'ICANN des politiques mondiales relatives aux noms de domaine de premier niveau géographiques. Il s'agit d'un forum permettant aux gestionnaires des domaines de premier niveau géographique de se rencontrer et de discuter des questions d'ordre mondial d'intérêt commun. La ccNSO sélectionne un des membres du Conseil d'administration.

5. ccTLD - Domaine de premier niveau géographique
Les ccTLD sont des domaines à deux caractères, tels que .UK (Royaume-Uni), .DE (Allemagne) et .JP (Japon) que l'on appelle des domaines de premier niveau géographiques (ccTLD) et qui correspondent à un pays, à un territoire ou à toute autre localisation géographique. Les règles et les politiques qui régissent l'enregistrement des

noms de domaine dans les ccTLD varient de manière significative. Les opérateurs de registre ccTLD limitent l'utilisation des ccTLD aux citoyens des pays concernés.

Pour plus d'informations sur les ccTLD et pour consulter la base de données complète des ccTLD avec leurs gestionnaires correspondants, veuillez consulter le site Internet http://www.iana.org/cctld/cctld.htm.

6. Données d'enregistrement des noms de domaine
Les données d'enregistrement des noms de domaine, également appelées « données d'enregistrement », concernent l'information qui est fournie par les titulaires de noms de domaine lors de l'enregistrement d'un nom de domaine, et qui est collectée par les bureaux d'enregistrement et les opérateurs de registre. Une partie de ces informations est disponible pour le public. Les éléments de données nécessaires pour l'interaction entre les bureaux d'enregistrement de noms de domaine génériques de premier niveau (gTLD) accrédités par l'ICANN et les titulaires de noms de domaine sont spécifiés dans le RAA en vigueur. Dans le cas des domaines de premier niveau géographiques (ccTLD), les opérateurs de ces TLD établissent leurs propres politiques relatives à la collecte et l'affichage des informations d'enregistrement ou suivent celles de leurs gouvernements.

7. Nom de domaine
En tant que composante du système des noms de domaine, les noms de domaine identifient les ressources du Protocole Internet telles qu'un site Internet.

8. DNS - Système des noms de domaine
Le « DNS » fait référence au système des noms de domaine sur Internet. Le système des noms de domaine (DNS) permet aux utilisateurs de se repérer plus facilement sur Internet. Chaque ordinateur connecté à l'Internet possède une adresse unique, comparable à un numéro de téléphone, qui se compose d'une chaine numérique relativement complexe, appelée « adresse IP » (IP signifiant « Protocole Internet »). Les adresses IP sont difficiles à mémoriser. Le DNS facilite l'utilisation de l'Internet en permettant le remplacement de cette adresse IP obscure par une chaîne alphabétique familière (le « nom de domaine »). Ainsi, au lieu de taper 207.151.159.3, vous pouvez saisir www.internic.net. C'est un procédé « mnémonique » qui facilite la mémorisation des adresses.

9. EPDP - Processus accéléré d'élaboration de politiques de la GNSO
Un ensemble d'étapes formelles, telles que définies dans les statuts constitutifs de l'ICANN, destinées à orienter la mise en place, l'examen interne et externe, l'établissement d'un calendrier et l'approbation des politiques nécessaires pour coordonner le système mondial d'identificateurs uniques de l'Internet. Un EPDP peut être lancé par le conseil de la GNSO uniquement dans les circonstances particulières suivantes : (1) aborder une problématique de politique, étroitement définie, qui a été identifiée et cadrée soit après l'adoption par le Conseil d'administration de l'ICANN

d'une recommandation de la GNSO en matière de politique, soit après la mise en œuvre d'une telle recommandation adoptée ; ou (2) fournir une recommandation supplémentaire en matière de politique sur une problématique de politique spécifique dont la portée a été considérablement déterminée précédemment de manière à ce qu'une information exhaustive existe déjà sur le contexte pertinent, par ex. (a) dans un rapport thématique sur un PDP potentiel n'ayant pas été lancé ou (b) dans le cadre d'un PDP précédent n'ayant pas été complété ou (c) à travers d'autres projets tels que le processus d'orientation de la GNSO.

10. GAC - Comité consultatif gouvernemental
Le GAC est un comité consultatif intégré par des représentants de gouvernements nationaux, des représentants d'organisations gouvernementales multinationales, d'organisations établies par des traités et des représentants de différentes économies. Sa mission est de conseiller le Conseil d'administration de l'ICANN sur des questions qui font l'objet d'inquiétudes de la part des gouvernements. Le GAC constitue un forum de discussion sur des inquiétudes ou des intérêts partagés par les gouvernements, y compris les intérêts des consommateurs. En sa qualité de comité consultatif, le GAC ne possède aucune autorité légale pour agir au nom de l'ICANN, mais il présente ses conclusions et ses recommandations au Conseil d'administration de l'ICANN.

11. Règlement général sur la protection de données (RGPD).
Le Règlement général sur la protection des données (UE) 2016/679 (RGPD) est un règlement de la loi de l'Union européenne relatif à la protection des données et de la vie privée pour toutes les personnes au sein de l'Union (EU) et de l'espace économique européen (EEE). Il aborde également l'exportation des données à caractère personnel en dehors du territoire de l'Union européenne (UE) et de l'espace économique européen (EEE).

12. GNSO - Organisation de soutien aux noms génériques
Organisation de soutien chargée d'élaborer et de recommander au Conseil d'administration de l'ICANN des politiques de fond liées aux domaines génériques de premier niveau. Elle est intégrée par des représentants des opérateurs de registre gTLD, des bureaux d'enregistrement gTLD, des organismes de protection des droits de propriété intellectuelle, des fournisseurs de services Internet, des entreprises et des organisations non commerciales.

13. Domaine générique de premier niveau (gTLD)
« gTLD » désigne le(s) domaine(s) de premier niveau du DNS délégué(s) par l'ICANN en vertu d'un contrat de registre qui est pleinement en vigueur, à l'exception des TLD géographiques (ccTLD) ou des TLD géographiques étant des noms de domaine internationalisés (IDN).

14. Groupe des représentants des opérateurs de registre (RySG)

Le Groupe des représentants des opérateurs de registre (RySG) est une entité reconnue au sein de l'Organisation de soutien aux extensions génériques (GNSO) constituée conformément à l'article 5 du chapitre X (septembre 2009) des statuts constitutifs de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN).

Le rôle principal du RySG consiste à représenter les intérêts des opérateurs de registre des gTLD (ou les sponsors dans les cas de gTLD parrainés) (« Opérateurs de registre ») (i) ayant passé un contrat avec l'ICANN pour fournir des services de registre à l'appui d'un ou plusieurs gTLD ; (ii) qui acceptent, dans ce contrat, de respecter les politiques de consensus ; et (iii) qui choisissent volontairement d'être membres du RySG. Le RySG est ouvert aux groupes d'intérêts visés au chapitre IV. Le RySG transmet ses points de vue au conseil de la GNSO et au Conseil d'administration de l'ICANN, en mettant l'accent particulièrement sur les politiques consensuelles de l'ICANN qui ont trait à l'interopérabilité, la fiabilité technique et le fonctionnement stable de l'Internet ou du système des noms de domaine.

15. ICANN - Société pour l'attribution des noms de domaine et des numéros sur Internet

L'ICANN est une association internationale de droit privé à but non lucratif qui est chargée de l'allocation de l'espace des adresses du Protocole Internet (IP), d'attribuer des identificateurs de protocole, de gérer le système de noms de domaine de premier niveau génériques (gTLD) et géographiques (ccTLD), et d'assurer les fonctions de gestion du système de serveurs racines. Ces services étaient initialement assurés dans le cadre d'un contrat avec le gouvernement américain par l'IANA (Autorité chargée de la gestion de l'adressage sur Internet) et d'autres organismes. L'ICANN assume à présent les fonctions de l'IANA. En tant que partenariat public-privé, l'ICANN a pour mission de préserver la stabilité opérationnelle de l'Internet, de promouvoir la concurrence, d'assurer une vaste représentation des communautés Internet à l'échelle mondiale et d'élaborer des politiques relatives à sa mission moyennant des processus ascendants basés sur le consensus.

16. Unité constitutive des représentants de la propriété intellectuelle (IPC)

L'Unité constitutive des représentants de la propriété intellectuelle représente les points de vue et les intérêts de la communauté de la propriété intellectuelle dans le monde entier, avec un accent particulier sur les marques de commerce, les droits d'auteur, les droits de propriété intellectuelle connexes et leur effet et leur interaction avec le système des noms de domaine. L'IPC est l'un des groupes constitutifs de l'Organisation de soutien aux extensions génériques (GNSO), chargée de conseiller le Conseil d'administration de l'ICANN sur les questions de politique relatives à la gestion du système des noms de domaine.

17. Unité constitutive des fournisseurs de services Internet et de services de connectivité (ISPCP)

L'Unité constitutive des fournisseurs de services Internet et de services de connectivité est une unité constitutive de la GNSO. Elle a pour objet de s'acquitter des rôles et responsabilités qui sont créés par les statuts constitutifs, règles ou politiques pertinents de l'ICANN et de la GNSO au fur et à mesure que l'ICANN mène à bien ses activités d'organisation. L'ISPCP veille à ce que les points de vue des fournisseurs de services Internet et de services de connectivité contribuent à la réalisation des buts et objectifs de l'ICANN.

18. Serveur de nom

Un serveur de nom est une composante du DNS qui stocke des informations sur une zone (ou plusieurs zones) de l'espace de noms du DNS.

19. Groupe des représentants des entités non commerciales (NCSG)

Le Groupe des représentants des entités non commerciales (NCSG) est l'un des groupes de représentants de la GNSO. Le Groupe des représentants des entités non commerciales (NCSG) a pour objet de représenter, à travers ses représentants élus et ses unités constitutives, les intérêts et les préoccupations des titulaires de noms de domaine non commerciaux et des utilisateurs Internet non commerciaux de domaines génériques de premier niveau (gTLD). Il est le porte-parole et le représentant, dans les processus de l'ICANN, des organisations à but non lucratif qui servent des intérêts non commerciaux ; des services à but non lucratif tels que l'éducation, la philanthropie, la protection des consommateurs, l'organisation communautaire, la promotion des arts, la défense des politiques d'intérêt public, le bien-être des enfants, la religion, la recherche scientifique et les droits de l'homme ; les préoccupations liées aux logiciels d'intérêt public ; des familles ou individus qui enregistrent les noms de domaine pour un usage personnel non commercial; et les utilisateurs de l'Internet qui sont principalement intéressés aux aspects non commerciaux et d'intérêt public des politiques de noms de domaine.

20. Procédure de règlement de litiges après délégation (PDDRP)

Les procédures de règlement de litiges après délégation ont été élaborées pour fournir aux personnes lésées par la conduite d'un nouvel opérateur de registre gTLD, une manière alternative de se plaindre de cette conduite. Ces procédures de règlement de litiges sont toutes administrées par des fournisseurs externes à l'ICANN et peuvent exiger que les plaignants prennent des mesures concrètes pour régler leurs problèmes avant de déposer une plainte officielle. Un panel d'experts déterminera si un opérateur de registre est en faute et recommandera des remèdes à l'ICANN.

21. Nom enregistré

L'expression « Nom enregistré » fait référence à un nom de domaine figurant dans le domaine d'un gTLD qui est composé de deux (2) ou plusieurs niveaux (par exemple : john.smith.name), pour lequel un opérateur de registre de gTLD (ou un affilié ou sous-contractant engagé dans la prestation de services de registre) maintient les données dans une base de données de registres, organise ledit maintien ou perçoit des revenus de ce maintien. Un nom figurant dans une base de données de registre peut être un

nom de domaine enregistré même s'il n'apparait pas dans un fichier de zone (par exemple : un nom de domaine enregistré, mais inactif).

22. Bureaux d'enregistrement
Le terme « bureau d'enregistrement », lorsqu'il apparaît sans majuscule, fait référence à une personne ou à une entité qui s'engage par contrat avec les titulaires des noms de domaine enregistrés et un opérateur de registres, et qui collecte des données d'enregistrement sur les titulaires des noms de domaine enregistrés et envoie des informations sur l'enregistrement afin qu'elles puissent être saisies dans la base de données des registres.

23. Groupe des représentants des bureaux d'enregistrement (RrSG)
Le Groupe des représentants des bureaux d'enregistrement est l'un des nombreux groupes de représentants au sein de la communauté de l'ICANN, et est l'organe représentatif des bureaux d'enregistrement. Il s'agit d'un groupe diversifié et actif qui veille à ce que les intérêts des bureaux d'enregistrement et de leurs clients soient efficacement protégés. Nous vous invitons à en savoir plus sur les bureaux d'enregistrement de noms de domaine accrédités et sur le rôle important qu'ils jouent dans le système des noms de domaine.

24. Opérateur de registre
Un « opérateur de registre » est la personne physique ou morale couramment responsable, conformément au contrat conclu entre l'ICANN (ou son cessionnaire) et cette/ces personne(s) physique(s) ou morale(s) ou, si ce contrat est résilié ou expiré, conformément à un contrat conclu entre le gouvernement des États-Unis et cette/ces personne(s) physique(s) ou morale(s), pour la prestation des services de registre concernant un gTLD spécifique.

25. Service d'annuaire de données d'enregistrement (RDDS)
Le service d'annuaire de données d'enregistrement des noms de domaine, ou RDDS, fait référence au(x) service(s) proposé(s) par les opérateurs de registre et les bureaux d'enregistrement pour permettre l'accès aux données d'enregistrement des noms de domaine.

26. Procédure de règlement de litiges relatifs à des restrictions à l'enregistrement (RRDRP)
La procédure de règlement de litiges relatifs à des restrictions à l'enregistrement (RRDRP) a pour objet d'aborder des circonstances dans lesquelles un opérateur de registre d'un nouveau gTLD communautaire a dévié des restrictions à l'enregistrement prévues dans le contrat de registre.

27. SO - Organisations de soutien

Les SO se composent de trois organes consultatifs spécialisés, chargés de conseiller le Conseil d'administration de l'ICANN sur des questions relatives aux noms de domaine (GNSO et CCNSO) et aux adresses IP (ASO).

28. SSAC - Comité consultatif sur la sécurité et la stabilité
Comité consultatif constitué par des experts techniques issus de l'industrie et du secteur académique, ainsi que par des opérateurs des serveurs racine de l'Internet, des bureaux d'enregistrement et des registres TLD qui conseille le Conseil d'administration de l'ICANN.

29. TLD - Domaine de premier niveau
Les TLD sont les noms situés au sommet de la hiérarchie de nommage du DNS. Dans les noms de domaine, ils représentent la chaîne de caractères qui suit le dernier « . » (le plus à droite). C'est le cas de « net » dans http://www.example.net. Le gestionnaire d'un TLD contrôle les noms de second niveau qui sont reconnus dans ce TLD. Les gestionnaires du « domaine racine » ou de la « zone racine » contrôlent les TLD qui sont reconnus par le DNS. Les TLD couramment utilisés sont, entre autres : .COM, .NET, .EDU, .JP, .DE, etc.

30. Politique de règlement uniforme de litiges relatifs aux noms de domaine (UDRP)
La politique de règlement uniforme de litiges relatifs aux noms de domaine (UDRP) est un mécanisme de protection des droits qui précise les procédures et les règles appliquées par les bureaux d'enregistrement dans le cadre de litiges survenant au cours de l'enregistrement et l'utilisation des noms de domaine gTLD. L'UDRP est une procédure administrative obligatoire visant surtout à résoudre des réclamations relatives à l'enregistrement malveillant ou de mauvaise foi de noms de domaine. Cette politique ne s'applique qu'aux litiges entre les titulaires de noms de domaine et les tiers, pas aux litiges entre un bureau d'enregistrement et son client.

31. Système uniforme de suspension rapide (URS)
Le système uniforme de suspension rapide est un mécanisme de protection des droits qui complète la Politique de règlement uniforme de litiges relatifs aux noms de domaine (UDRP) en vigueur en offrant aux détenteurs de droits une méthode plus efficace et économique pour résoudre les cas incontestables d'abus.

32. WHOIS
Le protocole WHOIS est un protocole Internet utilisé pour interroger des bases de données afin d'obtenir des informations sur l'enregistrement d'un nom de domaine (ou d'une adresse IP). Le protocole WHOIS a été initialement spécifié dans le RFC 954, publié en 1985. La spécification actuelle de ce protocole est décrite dans le document RFC 3912. Les contrats relatifs aux gTLD passés entre l'ICANN et les bureaux d'enregistrement et les opérateurs de registre exigent à ces derniers de permettre l'accès public aux données sur les noms enregistrés par le biais de pages Web interactives et des services WHOIS du port 43. Ces données, dites généralement «

données WHOIS » comprennent des éléments tels que la date de création et d'expiration des enregistrements de domaines, les serveurs de noms, l'information de contact du titulaire de nom de domaine ainsi que des représentants techniques et administratifs.

Les services WHOIS sont typiquement utilisés pour identifier les propriétaires de domaines à des fins commerciales et pour identifier les parties capables de corriger des problèmes techniques associés au domaine enregistré.

Annexe A – Système normalisé d'accès et de divulgation de données d'enregistrement non publiques – Informations de contexte

DESCRIPTION DE LA PROBLÉMATIQUE ET/OU QUESTIONS DE LA CHARTE

Extrait de la charte de l'équipe responsable de l'EPDP :
(a) Finalité de l'accès aux données : quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?

a1) Quelles sont les fins légitimes des tiers pour accéder aux données d'enregistrement en vertu de la législation applicable ?
a2) Quelles sont les bases juridiques existantes pour soutenir cet accès ?
a3) Quels sont les critères d'éligibilité pour l'accès aux données d'enregistrement non publiques ?
a4) Ces parties ou groupes sont-ils composés de différents types de demandeurs tiers ?
a5) À quels éléments de données chaque utilisateur ou groupe devrait-il avoir accès ?
a6) Dans quelle mesure est-il possible de déterminer un ensemble d'éléments de données et la portée potentielle (volume) pour des tiers et/ou des fins spécifiques ?
a7) Comment le RDAP, qui est techniquement compétent, peut-il permettre aux opérateurs de registre/bureaux d'enregistrement d'accepter les jetons d'accréditation et l'objet de la requête ? Une fois que les modèles d'accréditation seront développés par les accréditeurs appropriés et approuvés par les autorités juridiques compétentes, comment pourrons-nous nous assurer que le RDAP sera techniquement compétent et prêt à accepter, enregistrer et répondre au jeton du requérant accrédité ?

(b) Données d'identification – Quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?

b1) Comment les données d'identification seront-elles accordées et gérées ?
b2) Qui est responsable de les fournir ?
b3) Comment ces données d'identification seront-elles intégrées dans les systèmes techniques des bureaux d'enregistrement/opérateurs de registre ?

(c) Conditions d'accès et conformité aux conditions d'utilisation – Quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?

c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?

c2) Quelles règles/politiques régiront l'utilisation des données par les utilisateurs une fois qu'ils y auront accédé ?
c3) Qui sera responsable de l'établissement et de l'application de ces règles/politiques ?
c4) Le cas échéant, quelles sanctions ou pénalités seront imposées à un utilisateur pour l'utilisation malveillante des données, y compris les futures restrictions à l'accès ou à la rémunération des personnes concernées dont les données ont été utilisées à des fins malveillantes, outre les sanctions déjà prévues par la législation applicable ?
c5) Les parties contractantes seront-elles au courant des données auxquelles on accède et sur la façon dont elles sont utilisées ?
c6) Les personnes concernées ont-elles le droit de savoir quand et comment leurs données sont consultées et utilisées ?
c7) Comment un modèle d'accès tiers peut-il tenir compte des différentes exigences relatives à la notification des personnes concernées vis-à-vis de la divulgation de leurs données ?

De l'annexe à la Spécification temporaire :

- Élaborer des méthodes pour fournir aux plaignants potentiels utilisant l'URS et l'UDRP un accès suffisant aux données d'enregistrement à l'appui des dépôts de plaintes de bonne foi.
- Assurer que les limitations en termes de volume de requêtes envisagées dans le cadre d'un programme d'accréditation soient en équilibre avec les besoins réels de référence croisée.
- Confidentialité des requêtes pour des données d'enregistrement par les autorités d'application de la loi.
- Conformément à l'article 4.4, le travail continu de la communauté pour élaborer un modèle d'accréditation et d'accès qui respecte le RGPD, tout en reconnaissant la nécessité d'obtenir des conseils supplémentaires du groupe de travail « Article 29 »/Comité européen de la protection des données.
- Élaborer un processus cohérent permettant d'assurer l'accès continu aux données d'enregistrement, y compris les données non publiques, aux utilisateurs ayant un but légitime, jusqu'au moment où un mécanisme final d'accréditation et d'accès soit pleinement opérationnel et que cela soit obligatoire pour toutes les parties contractantes.

Rapport final de l'étape 1 de l'équipe responsable de l'EPDP :

Recommandation 3 de l'équipe responsable de l'EPDP.
Conformément à la charte de l'équipe responsable de l'EPDP et en ligne avec la finalité 2, maintenant que la série de questions de base soulevées dans la charte a été traitée, l'équipe responsable de l'EPDP s'engage à faire une recommandation concernant un modèle standard pour la divulgation légitime de données d'enregistrement non

publiques (désigné dans la charte sous le nom d'« accès normalisé »). Il s'agira notamment de répondre à des questions telles que :

- L'adoption d'un tel système serait-elle judicieuse ?
- Quelles sont les fins légitimes des tiers pour accéder à des données d'enregistrement ?
- Quels sont les critères d'éligibilité pour l'accès aux données d'enregistrement non publiques ?
- Ces parties ou groupes sont-ils composés de différents types de requérants tiers ?
- À quels éléments de données un utilisateur ou une partie devraient-ils avoir accès ?

Dans ce contexte, l'équipe responsable de l'EPDP examinera, entre autres, la divulgation en cas de violation de propriété intellectuelle et en cas d'utilisation malveillante du DNS. Il y a lieu de confirmer que la divulgation à des fins légitimes n'est pas incompatible avec les finalités pour lesquelles ces données ont été recueillies.

Questions relatives aux politiques de TSG

1. Résultats de l'EPDP, ou d'autres initiatives de politique, concernant l'accès aux données d'enregistrement de noms de domaine gTLD non publiques.
2. Identification et sélection de fournisseurs d'identité (si ce choix est fait) qui puissent octroyer des données d'identification pour leur utilisation dans le système.[45]
3. Description des qualifications générales d'un requérant autorisé à accéder aux données d'enregistrement de nom de domaine gTLD non publiques, par exemple quels types de requérants accèdent à quels champs des données d'enregistrement de nom de domaine gTLD non publiques (« la politique d'autorisation »).
4. Indiquer si tous les requérants en général ou seule une catégorie particulière de requérants peut télécharger les journaux de leur activité.
5. Description des exigences de conservation des données imposées à chaque composant du système.
6. Description des exigences de niveau de service (SLR) pour chaque composante du système, y compris si ces SLR et les évaluations des opérateurs de composantes par rapport à eux sont rendues publiques, et pour traiter les plaintes concernant l'accès.
7. Spécification des causes légitimes du refus d'une requête.
8. Description de la prise en charge de la corrélation via une requête de pseudo-anonymat comme décrit à la section 7.2.

[45] Plusieurs ont fait remarquer que la réponse à cette question pourrait ne pas être dans la portée de l'équipe responsable de l'EPDP.

9. Description de la sélection d'un modèle d'acteur comme décrit à la section 8 et découverte des composantes et des services appropriés pris en charge comme décrit aux sections 10.1 à 10.5.
10. Description des conditions, le cas échéant, dans lesquelles les demandes seraient divulguées aux parties contractantes (CP).
11. Fourniture d'une analyse juridique concernant la responsabilité des opérateurs des différentes composantes du système.
12. Description d'une procédure de règlement des plaintes concernant des divulgations inappropriées et, par conséquent, d'une politique d'utilisation acceptable.

LIVRABLE ATTENDU

Recommandations de politique pour un modèle normalisé de divulgation/accès légitime de données d'enregistrement non publiques

LECTURE GÉNÉRALE REQUISE

Description	Lien	Fondements du caractère obligatoire
Éléments cadre pour le modèle d'accès unifié pour un accès continu aux données WHOIS complètes (18 juin 2018)	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf	
Modèle préliminaire d'accréditation et d'accès aux données WHOIS non publiques (BC/IPC)	Modèle version 1.7 du 23 juillet 2018	
Modèle d'accès aux données des titulaires de noms de domaine différencié de Palage (alias Philly Special)	Modèle d'accès aux données des titulaires de noms de domaine différencié de Palage (alias Philly Special) - version 2.0 du 30 mai 2018	

Modèle d'accès unifié pour un accès continu aux données WHOIS complètes - comparaison des modèles présentés par la communauté (18 juin 2018)	https://www.icann.org/en/system/files/files/draft-unified-access-model-summary-elements-18jun18-en.pdf	
Opinion du groupe de travail Article 29 sur l'application des principes de protection des données 2/2003 aux répertoires WHOIS (2003)	https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf	
Section 4c du rapport de l'EWG, « Principes d'accréditation des utilisateurs du RDS » (juin 2014)	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf	
Recherche de l'EWG – Demande d'information concernant l'accréditation des utilisateurs du RDS	https://community.icann.org/download/attachments/45744698/EWG%20USER%20ACCREDITATION%20RFI%20SUMMARY%2013%20March%202014.pdf	
1e partie : Le principe en est le suivant : RDAP – 10 mars 2019	https://64.schedule.icann.org/meetings/963337	
Deuxième partie : comprendre le RDAP et son rôle potentiel dans la politique du RDDS - 13 mars 2019	https://64.schedule.icann.org/meetings/961941	
Modèle technique d'accès aux données d'enregistrement non publiques proposé par le Groupe d'étude technique sur l'accès aux données d'enregistrement non publiques (30 avril 2019)	TSG01, Modèle technique d'accès aux données d'enregistrement non publiques	

Rapport final sur les questions liées à l'accréditation des services d'enregistrement fiduciaire et d'anonymisation (7 décembre 2015) ● Définitions - pages 6 à 8 ● Annexe B – Cadre de divulgation illustratif applicable aux requêtes de divulgation des titulaires de droits de propriété intellectuelle – pages 85 à 93 ● Contrat d'accréditation des fournisseurs de services d'anonymisation et d'enregistrement fiduciaire	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	

MISES À JOUR INFORMATIVES À APPORTER

Thème	Présentateurs possibles	Importance
RDAP – Questions/réponses suivant la révision des séances de l'ICANN65	Francisco Arias, organisation ICANN	Garantir une compréhension commune du fonctionnement et des capacités du RDAP

DÉPENDANCES

Description de la dépendance	Dépendance	Délai prévu ou recommandé
La négociation et la finalisation des contrats de protection des données exigés aux termes du rapport de l'étape 1 sont une condition préalable pour une bonne partie du travail de l'étape 2 (suggéré par l'ISPCP)	Organisation ICANN / Parties contractantes	

DÉLAI ET APPROCHE PROPOSÉS

Introduction
L'objectif de l'équipe responsable de l'EPDP est d'élaborer et d'accorder des recommandations de politique pour le partage des données d'enregistrement non publiques[46] avec les parties requérantes (Système normalisé d'accès et de divulgation des données d'enregistrement non publiques).

En attendant que des garanties juridiques satisfaisantes pour les parties concernées soient fournies, l'élaboration des recommandations de politique pour un système normalisé de divulgation et d'accès sera indépendante des modalités du système.

Parallèlement, l'équipe responsable de l'EPDP dans son ensemble devrait collaborer avec l'organisation ICANN au développement de questions politiques qui aideront à éclairer les discussions avec les APD qui ont pour objectif de déterminer quel modèle de système normalisé de divulgation serait entièrement conforme au RGPD, applicable et répondrait ou allégerait la responsabilité juridique des parties contractantes.

Liste non exhaustive des sujets à traiter :

- Terminologie et définitions de travail
- Besoin de conseils juridiques
- Exigences, y compris la définition des groupes d'utilisateurs et des critères et contenus des requêtes
- Publication du processus, des critères et des requêtes de contenus exigées
- Délais du processus

[46] Rapport final de l'étape 1 de l'équipe responsable de l'EPDP : On entend par « données d'enregistrement » les éléments de données identifiés à l'annexe D [du rapport final de l'étape 1 de l'EPDP], recueillis auprès d'une personne physique et morale dans le cadre de l'enregistrement d'un nom de domaine.

- Réception de l'accusé de réception
- Accréditation
- Authentification et autorisation
- Finalités de la divulgation par des tiers
- Fondement juridique de la divulgation
- Politiques acceptables en matière d'utilisation
- Conditions d'utilisation / accords de divulgation, y compris le respect des exigences légales
- Politiques en matière de vie privée
- Politique applicable aux requêtes
- Conservation et destruction des données
- Conventions de service
- Viabilité financière

Approche

Déterminer d'emblée :

a) Terminologie et définitions de travail
b) Identifier les conseils juridiques nécessaires (notez qu'il s'agit également d'une activité continue sur tous les sujets).

Ordre logique possible pour traiter les sujets restants :

c) Définir des groupes d'utilisateurs, des critères et des objectifs / fondements juridiques par groupe d'utilisateurs
↓
d) Authentification / autorisation / accréditation des groupes d'utilisateurs
↓
e) Critères / contenu des requêtes par groupe d'utilisateurs
↓
f) Politique applicable aux requêtes
↓
g) Réception de l'accusé de réception, y compris les délais
↓
h) Exigences / attentes en matière de réponse, y compris les délais / SLA
↓
i) Politiques acceptables en matière d'utilisation
↓
j) Conditions d'utilisation / accords de divulgation / politiques en matière de vie privée
↓
k) Conservation et destruction des données

l) Sujet global à considérer : viabilité financière

Vous trouverez ci-dessous de plus amples informations sur chacun de ces sujets. Pour accéder à chaque section, veuillez utiliser les liens ci-dessous :

Après avoir rempli la présente feuille de travail et d'autres, chaque sujet (y compris les sujets de l'étape 1) et sa portée de travail formeront la base d'un plan de travail global prévu. Certains sujets peuvent être traités en parallèle, tandis que d'autres peuvent avoir des dépendances avec d'autres travaux avant que des délibérations plus éclairées puissent être menées. Un temps fixe sera attribué aux délibérations de chaque sujet, à la formulation des conclusions possibles et / ou des recommandations éventuelles aux questions de politique. Les conclusions ou les recommandations qui obtiennent un niveau général de soutien passeront par un examen plus approfondi et seront peaufinés pour un rapport initial. L'objectif est d'atteindre des niveaux de consensus sur la ou les propositions, lorsque cela sera possible avant leur publication.

a) Sujet : Terminologie et définitions de travail

Objectif : Afin de garantir que les termes utilisés dans le contexte de cette discussion soit compris de la même manière et éviter toute confusion, l'équipe responsable de l'EPDP doit convenir un ensemble de définitions de travail. Il est entendu que ces définitions de travail servent simplement à clarifier la terminologie utilisée, qu'elles ne visent en aucun cas à restreindre la portée des travaux ou à prédéterminer le résultat. Il est entendu que ces définitions de travail devront être revues et révisées, au besoin, à la fin du processus.

Documents à examiner :

- Terminologie utilisée dans le RGPD et dans d'autres lois relatives à la protection des données
- Rapport final sur les questions liées à l'accréditation des services d'enregistrement fiduciaire et d'anonymisation (7 décembre 2015) - Définitions - pages 6 à 8

Question connexe de la carte heuristique : Aucune

Mise en œuvre connexe de l'étape 1 de l'EPDP : À confirmer - la mise en œuvre de la Recommandation 18 peut inclure des définitions qui pourraient devoir être prises en compte dans les délibérations de l'étape 2 de l'équipe responsable de l'EPDP.

Tâches :

- Confirmer s'il y a des définitions censées être élaborées ou appliquées à la mise en œuvre de la Recommandation 18 (personnel)
- Développer une première version préliminaire des définitions de travail. (Personnel)
- L'équipe responsable de l'EPDP doit l'évaluer et fournir ses commentaires (EPDP)
- Obtenir un accord sur l'ensemble de définitions de base (EPDP)
- Tenir à jour le document de travail des définitions par le biais de délibérations (tous)

Date cible d'achèvement : 30 Mai 2019

b) Sujet : Questions juridiques

Objectif : identifier les questions juridiques qui sont essentielles pour aider à éclairer les délibérations de l'équipe responsable de l'EPDP sur ce sujet.

Questions soumises à ce jour :

Question	État	Propriétaire
1. Il y a lieu de confirmer que la divulgation à des fins légitimes n'est pas incompatible avec les finalités pour lesquelles ces données ont été recueillies.	**EN ATTENTE** Le conseiller juridique de l'étape 2 a signalé cette question comme prématurée à l'heure actuelle et la marquera comme « en attente ». La question sera réexaminée une fois que l'équipe responsable de l'EPDP aura identifié les finalités de la divulgation.	
2. Répondre à la question du contrôle et de la base juridique pour un système d'accès normalisé aux données d'enregistrement non publiques, en supposant un cadre technique conforme au TSG, et d'une manière qui aborde suffisamment des questions liées à la responsabilité et à l'atténuation des risques dans le but de réduire les risques de responsabilité pour les parties contractantes à travers l'adoption d'un système d'accès normalisé (IPC)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	

3. Des conseils juridiques devraient être demandés sur la possibilité d'avoir un système qui autorise la divulgation en fonction de l'accréditation. (ISPCP)	**EN ATTENTE** Le conseiller juridique de l'étape 2 a signalé cette question comme prématurée à l'heure actuelle et la marquera comme « en attente ». La question sera réexaminée une fois que l'équipe responsable de l'EPDP aura identifié les finalités de la divulgation.	
4. La question de la divulgation à des organismes d'application de la loi non membres de l'UE, fondée sur l'article 6 du RGPD, devrait être présentée à un avocat. (ISPCP)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 cherche des précisions de l'auteur au sujet de cette question et, une fois que les orientations et / ou le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
5. Un modèle centralisé d'accès/de divulgation (dans lequel une seule entité est responsable de la réception des demandes de divulgation, de l'exécution du test d'équilibrage, de la vérification de l'accréditation, de la réponse aux requêtes,	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler	

etc.) peut-il être conçu de manière à limiter dans la mesure du possible la responsabilité des parties contractantes ? IE - peut-on dire que l'entité centralisée peut être en grande partie (sinon entièrement) responsable de l'obligation associée à la divulgation (y compris l'accréditation et l'autorisation) et que la responsabilité des parties contractantes peut être limitée aux activités strictement associées à d'autres traitements non liés à la divulgation, par exemple, la collecte et le transfert sécurisé des données ? Si oui, qu'est-ce qui doit être pris en compte/articulé dans la politique pour y répondre ? (ISPCP)	cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
6. Dans le contexte d'un SSAD, en plus de déterminer sa propre base légale pour la divulgation de données, la personne ayant envoyé la requête (l'entité qui héberge les données requises) a-t-elle besoin d'évaluer la base légale du demandeur tiers ? (Question du GAC/IPC de l'ICANN65)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
7. Dans quelle mesure, le cas échéant, les parties contractantes sont-elles responsables lorsqu'un tiers fausse son usage prévu des données et comment réduire cette responsabilité ? (BC)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la	

	question devrait être transmise à un conseiller juridique externe.	
8. La BC propose que l'EPDP divise la Finalité 2 en deux buts distincts : • Permettre à l'ICANN de maintenir la sécurité, la stabilité et la résilience du système de noms de domaine conformément à la mission et aux statuts constitutifs de l'ICANN par le contrôle et le traitement des données d'enregistrement de gTLD. • Permettre à des tiers de s'attaquer à la protection des consommateurs, à la cybersécurité, à la propriété intellectuelle, à la cybercriminalité et à l'utilisation malveillante du DNS impliquant l'utilisation ou l'enregistrement de noms de domaine. Un conseiller juridique peut être consulté pour trancher la question de la reformulation de la Finalité 2 (comme indiqué ci-dessus) Est-il possible de consulter un conseiller juridique pour déterminer si la Finalité 2 reformulée (comme indiqué ci-dessus) est possible aux termes du RGPD ? Si la formulation ci-dessus n'est pas admissible, y a-t-il des suggestions que le conseiller juridique puisse faire pour améliorer la rédaction ? (BC)	**EN ATTENTE** Le conseiller juridique de l'étape 2 a signalé cette question comme prématurée à l'heure actuelle et la marquera comme « en attente ». La question sera réexaminée une fois que le conseil de la GNSO et le Conseil d'administration auront achevé leurs consultations sur : la Recommandation 1, Finalité 2.	
9. Une analyse juridique peut-elle être fournie sur la façon dont le test d'équilibrage prévu à l'alinéa 6(1)f) doit être effectué, et dans quelles circonstances l'alinéa 6(1)f) peut-il exiger un examen manuel d'une requête ? (BC)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été	

	examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
10. Si toutes les demandes ne bénéficient pas d'une révision manuelle, existe-t-il une méthodologie juridique permettant de définir des catégories de requêtes (par exemple, une réponse rapide à une attaque de logiciels malveillants ou la prise de contact avec un contrevenant IP non réactif) qui puissent être structurées pour réduire le besoin d'un examen manuel ? (BC)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
11. Est-il possible de consulter un conseiller juridique pour déterminer si le RGPD empêche l'accès à un volume plus élevé pour les professionnels de la cybersécurité dûment qualifiés ayant convenu des mesures de protection appropriées ? Si un tel accès n'est pas interdit, l'avocat peut-il fournir des exemples de mesures de protection (comme la pseudonymisation) qui devraient être prises en considération ? (BC)	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
12. Pour identifier l'alinéa 6(1)b) comme une finalité du traitement des données d'enregistrement, nous devons suivre l'avis de B&B selon lequel « il sera nécessaire	**EN VOIE DE REFORMULATION**	

d'exiger que le tiers spécifique ou du moins le traitement par le tiers soit, au moins de manière abstraite, déjà connu de la personne concernée au moment de la conclusion du contrat et que l'autorité de contrôle, en tant que partenaire contractuel, en informe la personne concernée avant le transfert au tiers » B&B devrait préciser pourquoi il estime que la seule justification pour divulguer le WHOIS est la prévention de l'utilisation malveillante du DNS. Sa conclusion au paragraphe 10 ne tient pas compte des autres finalités identifiées par la Recommandation 1 de l'EPDP et, en tout état de cause, devrait tenir compte de la récente reconnaissance de la communauté habilitée que l'ICANN a pour objectif général de : « Contribuer au maintien de la sécurité, de la stabilité et de la résilience du système de noms de domaine conformément à la mission de l'ICANN », qui est au cœur du rôle de l'ICANN en tant que « gardien » du système des noms de domaine ».	Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	
13. B&B devrait donner des conseils sur la mesure dans l'applicabilité de l'intérêt public comme justification, au titre de l'article 6(1) du RGPD, compte tenu de la reconnaissance par la communauté habilitée que : « En ce qui concerne la formulation de la Finalité 2, la Commission européenne reconnaît le rôle central et la responsabilité de l'ICANN pour assurer la sécurité, la stabilité et la résilience du système des noms de domaine de l'Internet et que pour ce faire, elle agit dans l'intérêt public ».	**EN VOIE DE REFORMULATION** Le conseiller juridique de l'étape 2 est en train de reformuler cette question et, une fois que le texte mis à jour aura été examiné, il déterminera si la question devrait être transmise à un conseiller juridique externe.	

Tâches :
- Déterminer les questions prioritaires pour les sujets liés à l'étape 2
- Convenir une approche et un processus d'approbation pour les questions qui surgissent tout au long des délibérations

Date cible d'achèvement : En cours

c) Sujet : Définir des groupes d'utilisateurs, des critères et des objectifs / fondements légitimes par groupe d'utilisateurs

Objectif :
- Définir les catégories de groupes d'utilisateurs qui peuvent demander la divulgation ou l'accès à des données d'enregistrement non publiques, ainsi que les critères qui devraient être appliqués pour déterminer si une personne ou une entité appartient à cette catégorie.
- Déterminer les finalités et les motivations légitimes par groupe d'utilisateurs pour le traitement des données
- Déterminer si et comment le cadre normalisé de l'étape 2 peut répondre aux demandes propres aux groupes à forte empreinte. Déterminer si les personnes qui ne correspondent à aucun des groupes d'utilisateurs identifiés peuvent toujours demander la divulgation ou l'accès par la mise en œuvre de la Recommandation 18 ou par d'autres moyens.

Questions connexes de la carte heuristique :

P1-Charter-a
(a) Finalité de l'accès aux données : quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?

a1) Quelles sont les fins légitimes des tiers pour accéder aux données d'enregistrement en vertu de la législation applicable ?
a2) Quelles sont les bases juridiques existantes pour soutenir cet accès ?
a3) Quels sont les critères d'éligibilité pour l'accès aux données d'enregistrement non publiques ?
a4) Ces parties ou groupes sont-ils composés de différents types de demandeurs tiers ?

Annexe à la Spécification temporaire :
3. Élaborer des méthodes pour fournir aux requérants potentiels des URS et des UDRP l'accès suffisant aux données d'enregistrement à l'appui du dépôt de plaintes de bonne foi.

Recommandations de l'étape 1
Recommandation 3 de l'équipe responsable de l'EPDP

- Quelles sont les fins légitimes des tiers pour accéder à des données d'enregistrement ?
- Quels sont les critères d'éligibilité pour l'accès aux données d'enregistrement non publiques ?
- Ces parties ou groupes sont-ils composés de différents types de requérants tiers ?

L'équipe responsable de l'EPDP demande que, lorsqu'elle entamera ses délibérations concernant un cadre d'accès unifié, un représentant du groupe de travail fournisse une mise à jour de l'état d'avancement des délibérations pour que l'équipe responsable de l'EPDP puisse déterminer si/comment les recommandations du groupe de travail peuvent avoir un impact sur l'examen de l'URS et de l'UDRP dans ce contexte.

Il est à noter que la finalité 2 est un espace réservé, en attendant que soit réalisé, au cours de l'étape 2 de cet EPDP, un travail complémentaire sur la question de l'accès; il serait à réexaminer à l'issue de l'étape 2. [note du personnel - liée aux finalités mais la Finalité 2 sera révisée est une fois que le travail de l'étape 2 aura été terminé]

TSG-Final-Q#3
3. Description des qualifications générales d'un requérant autorisé à accéder aux données d'enregistrement de nom de domaine gTLD non publiques, par exemple quels types de requérants accèdent à quels champs des données d'enregistrement de nom de domaine gTLD non publiques (« la politique d'autorisation »).

Documents à examiner :

Description	**Lien**	**Fondements du caractère obligatoire**
En fin juin 2017, l'ICANN a demandé aux parties contractantes et aux parties prenantes intéressées d'identifier les types d'utilisateurs et les finalités de l'accès aux éléments de données requis par les politiques et les contrats de l'ICANN. Les réponses individuelles reçues et une compilation des réponses sont fournies ci-dessous.	Organigramme des données, compilation des réponses reçues – version actuelle	Effort le plus récent pour identifier les types d'utilisateurs

Le rapport final de l'EWG présente un résumé non exhaustif des utilisateurs du système WHOIS actuel, y compris ceux dont les finalités sont constructives ou malicieuses. Conformément au mandat de l'EWG, tous ces utilisateurs ont été examinés pour identifier les futurs flux de travail existants et possibles, les parties prenantes et les données impliquées.	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf - pages 20 à 25	
Révision des finalités établies et fondement juridique identifié dans le cadre de l'étape 1 de l'équipe responsable de l'EPDP	https://gnso.icann.org/en/drafts/epdp-gtld-registration-data-specs-final-20feb19-en.pdf (pages 34 à 36 et 67 à 71)	
Dispositions pertinentes du RGPD	Dispositions pertinentes du RGPD - Consulter l'article 6(1), l'article 6(2) et le considérant 40	
Base légale de l'ICO pour le traitement de la page d'informations	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/	

Mise en œuvre connexe de l'étape 1 de l'EPDP :
Rien prévu

Tâches :

- Élaboration de la première liste de catégories de requérants en fonction des documents source. (Personnel)
- Réexaminer la liste des catégories de requérants et déterminer les critères d'éligibilité. (Tous)
- Élaborer des types et des scénarios d'utilisation malveillante pour formuler des cas d'utilisation afin de déterminer les exigences pour chaque requérant
- Déterminer les finalités et la base juridique par groupe d'utilisateurs pour le traitement de données (Tous)

- Déterminer si et comment le cadre normalisé de l'étape 2 peut répondre aux demandes propres aux groupes à forte empreinte. Déterminer si les personnes qui ne correspondent à aucun des groupes d'utilisateurs identifiés peuvent toujours demander la divulgation ou l'accès par la mise en œuvre de la Recommandation 18 ou par d'autres moyens. (Tous)
- Confirmer que toutes les questions posées dans la charte aient été abordées et documentées.

Date cible d'achèvement : 13 juin 2019
(Réexaminer la finalité 2 - une fois que le travail de l'étape 2 ait été complété)

d) Authentification / autorisation / accréditation des groupes d'utilisateurs

Objectif :

- Déterminer si l'authentification, l'autorisation et/ou l'accréditation des groupes d'utilisateurs devraient être requises
    - Est-il possible d'utiliser un modèle d'accréditation en complément ou avec ce qui est mis en œuvre dans le cadre de la Recommandation 18 de l'étape 1 de l'EPDP ?
- Si c'est le cas, établir des principes de politique pour l'authentification, l'autorisation et/ou l'accréditation, y compris pour répondre à des questions telles que :
    - Si un utilisateur authentifié requérant l'accès à des données WHOIS non publiques doit justifier son intérêt légitime pour chaque requête/demande individuelle ou non.
- Dans la négative, expliquer pourquoi et quelles en seraient les conséquences sur les requêtes de certains groupes d'utilisateurs, le cas échéant.

Questions connexes de la carte heuristique :

P1-Charter-a/b

(a) Finalité de l'accès aux données - Quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?
a7) Comment le RDAP, qui est techniquement compétent, peut-il permettre aux opérateurs de registre/bureaux d'enregistrement d'accepter les jetons d'accréditation et l'objet de la requête ? Une fois que les modèles d'accréditation seront développés par les accréditeurs appropriés et approuvés par les autorités juridiques compétentes, comment pourrons-nous nous assurer que le RDAP sera techniquement compétent et prêt à accepter, enregistrer et répondre au jeton du requérant accrédité ?

(b) Données d'identification – Quelles sont les questions de politique sans réponse qui guideront la mise en œuvre ?
b1) Comment les données d'identification seront-elles accordées et gérées ?
b2) Qui est responsable de les fournir ?
b3) Comment ces données d'identification seront-elles intégrées dans les systèmes techniques des bureaux d'enregistrement/opérateurs de registre ?

Annexe à la Spécification temporaire

1. Conformément à l'article 4.4, le travail continu de la communauté pour élaborer un modèle d'accréditation et d'accès qui respecte le RGPD, tout en reconnaissant la nécessité d'obtenir des conseils supplémentaires du groupe de travail « Article 29 »/Comité européen de la protection des données.

TSG-Final-Q#2

Identifier et sélectionner des fournisseurs d'identité (si ce choix est fait) qui puissent octroyer des données d'identification pour leur utilisation dans le système.

Documents à examiner :

Description	Lien	Fondements du caractère obligatoire
Identification et authentification dans le modèle du TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf pages 23 et 24	
Rapport final de l'EWG - Autorisation d'utilisation du contact RDS et Principes d'accréditation des utilisateurs du RDS	https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf page 39 à 40 et pages 62 à 67	
Cadre préliminaire pour un éventuel modèle d'accès unifié pour l'accès continu à l'intégrale des données WHOIS complètes - Comment les exigences d'authentification pour les utilisateurs légitimes seraient-elles conçues ?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf pages 9 à 10, 10 à 11, 18 et 23	

Mise en œuvre connexe de l'étape 1 de l'EPDP :
Rien prévu.

Tâches :

- Réviser les documents énumérés ci-dessus et discuter des perspectives sur l'authentification / l'autorisation (EPDP)
- Confirmer la définition des termes clés « autorisation », « accréditation » et « authentification »
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant

- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : ICANN 65

e) Critères / contenu des requêtes par groupe d'utilisateurs

Objectif : établir les exigences minimales en matière de politique, les critères et le contenu des requêtes par groupe d'utilisateurs, tel qu'indiqué à la section c.

Questions connexes de la carte heuristique :

P1-Charter-c
c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?

Documents à examiner :

Description	Lien	Fondements du caractère obligatoire
• Annexe B – Cadre de divulgation illustratif applicable aux requêtes de divulgation des titulaires de droits de propriété intellectuelle – pages 85 à 93 • Contrat d'accréditation des fournisseurs de services d'anonymisation et d'enregistrement fiduciaire	Rapport final sur les questions liées à l'accréditation des services d'enregistrement fiduciaire et d'anonymisation (7 décembre 2015)	
Exemple : Formulaire de requête et information de .DE	https://www.denic.de/en/service/whois-service/third-party-requests-for-holder-data/ https://www.denic.de/fileadmin/public/downloads/Domaindatenanfrage/Antrag_Domaindaten_Rechteinhaber_EN.pdf	

Exemple : Formulaire de requête de Nominet	https://s3-eu-west-1.amazonaws.com/nominet-prod/wp-content/uploads/2018/05/22101442/Data-request-form.pdf	

Mise en œuvre connexe de l'étape 1 de l'EPDP :

Recommandation 18 (mais NE requiert PAS la divulgation automatique d'information)

Information minimale exigée pour les requêtes raisonnables de divulgation légitime :

- l'identification du requérant et les informations à son sujet (y compris, la nature/le type d'entreprise ou de personne, les déclarations de procuration, le cas échéant) ;
- des informations sur les droits légaux du requérant ainsi que les fondements ou justifications particulières de la requête (par exemple, la base ou le motif de la requête ; pourquoi le requérant a-t-il besoin de ces données ?) ;
- l'affirmation que la requête est faite de bonne foi ;
- une liste des éléments de données requis par le requérant ainsi que la raison pour laquelle ces données se limitent à la nécessité ;
- l'engagement du requérant à traiter en toute licéité les données reçues en réponse à sa demande.

Tâches :

- Confirmer l'approche de mise en œuvre de la Recommandation 18
- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : ICANN 65

f) Politique applicable aux requêtes

Objectif : Définir les exigences minimales de politique pour la journalisation des requêtes, définir les contrôles appropriés pour la mise à disposition des journaux de requêtes et s'il devrait y avoir des limitations de requêtes pour les utilisateurs authentifiés et non authentifiés du SSAD.

- Comment l'accès aux données d'enregistrement non publiques sera-t-il limité afin de minimiser les risques d'accès et d'usages non autorisés (par exemple, en autorisant l'accès sur la base de requêtes spécifiques uniquement par opposition aux transferts groupés et/ou autres restrictions sur les recherches ou les services d'annuaire inversés, y compris des mécanismes visant à restreindre l'accès aux champs à ce qui est nécessaire pour atteindre la finalité légitime en question) ?
- La confidentialité des requêtes devrait-elle être prise en considération, par exemple par les organismes d'application de la loi ?
- Comment les limites des requêtes devraient-elles être équilibrées par rapport aux besoins réalistes de référencement croisé des enquêtes ?

Questions connexes de la carte heuristique :

P1-Charter-a
a7) Comment le RDAP, qui est techniquement compétent, peut-il permettre aux opérateurs de registre/bureaux d'enregistrement d'accepter les jetons d'accréditation et l'objet de la requête ? Une fois que les modèles d'accréditation seront développés par les accréditeurs appropriés et approuvés par les autorités juridiques compétentes, comment pourrons-nous nous assurer que le RDAP sera techniquement compétent et prêt à accepter, enregistrer et répondre au jeton du requérant accrédité ?

Annexe à la Spécification temporaire :
6 limitations en termes de volume de requêtes envisagées dans un programme d'accréditation équilibré contre les besoins réalistes de référencement croisé des enquêtes.
7 Confidentialité des requêtes pour les données d'enregistrement par les organismes d'application de la loi.

Documents à examiner :

Description	**Lien**	**Fondements du caractère obligatoire**
SSAC 101 - Rapport consultatif du SSAC sur l'accès aux données d'enregistrement de noms de domaine	https://www.icann.org/en/system/files/files/sac-101-en.pdf	Décrit les effets de la limitation du débit.

Mise en œuvre connexe de l'étape 1 de l'EPDP : Aucune.

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : ICANN 65

g) Réception de l'accusé de réception, délais y compris

Objectif : Définir les exigences de politique concernant les délais de l'accusé de réception et les exigences supplémentaires (le cas échéant) que l'accusé de réception devrait contenir.

Le cas échéant, quelles sont les exigences minimales normalisées de base en matière de réception des accusés de réception pour les bureaux d'enregistrement/opérateurs de registre ? Qu'en est-il des demandes « urgentes » et comment sont-elles définies ?

Questions connexes de la carte heuristique :

P1-Charter-c
c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?

Documents à examiner :

Description	**Lien**	**Fondements du caractère obligatoire**
Recommandation 18 du rapport final de l'étape 1 Délais et critères des réponses des bureaux d'enregistrement et des opérateurs de registre :	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-	

	specs-final-20feb19-en.pdf page 19	

Mise en œuvre connexe de l'étape 1 de l'EPDP : - Recommandation 18 :
Délais et critères des réponses des bureaux d'enregistrement et des opérateurs de registre -
Les bureaux d'enregistrement et les opérateurs de registre doivent raisonnablement tenir compte des demandes de divulgation légitime et y répondre :
• Le délai de réponse pour confirmer la réception d'une requête raisonnable de divulgation légitime. Sans retard injustifié, mais pas plus de deux (2) jours ouvrables suivant la réception, à moins que des circonstances avérées ne le permettent pas.

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : à déterminer

h) Exigences/attentes de réponse, y compris les délais/SLA

Objectif : Définir les exigences de politique concernant les exigences de réponse, y compris répondre à des questions telles que :

- Y compris répondre à des questions telles que :
  - si les données WHOIS complètes doivent être envoyées en réponse ou non lorsqu'un utilisateur authentifié exécute une requête.
  - quels devraient être les engagements SLA pour les réponses aux demandes d'accès/divulgation
  - quelles sont les exigences minimales pour les réponses aux requêtes, y compris le refus des requêtes ?

Questions connexes de la carte heuristique :

P1-Charter-a/c
a5) À quels éléments de données chaque utilisateur ou groupe devrait-il avoir accès en fonction de sa finalité ?

a6) Dans quelle mesure est-il possible de déterminer un ensemble d'éléments de données et la portée potentielle (volume) pour des tiers spécifiques et/ou finalités ?
c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?

Recommandation 3 de l'étape 1
À quels éléments de données un utilisateur ou une partie devraient-ils avoir accès ?

Annexe à la Spécification temporaire
2. Aborder la faisabilité d'exiger des contacts uniques pour avoir une adresse e-mail anonyme uniforme à travers les enregistrements de noms de domaine à un bureau d'enregistrement donné, tout en assurant la sécurité, la stabilité et le respect des exigences de la section 2.5.1 de l'annexe A.

TSG-Final-Q#6
Description des exigences de niveau de service (SLR) pour chaque composante du système, y compris si ces SLR et les évaluations des opérateurs de composantes par rapport à eux sont rendues publiques, et pour traiter les plaintes concernant l'accès.
TSG-Final-Q#7
Spécification des causes légitimes du refus d'une requête.
TSG-Final-Q#8
Description de la prise en charge de la corrélation via une requête de pseudo-anonymat comme décrit à la section 7.2.

Documents à examiner :

Description	**Lien**	**Fondements du caractère obligatoire**
Recommandation 18 du rapport final de l'étape 1 Délais et critères des réponses des bureaux d'enregistrement et des opérateurs de registre :	https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf page 19	

Rapport final sur les questions liées à l'accréditation des services d'enregistrement fiduciaire et d'anonymisation (7 décembre 2015) ● Annexe B – Cadre de divulgation illustratif applicable aux requêtes de divulgation des titulaires de droits de propriété intellectuelle – pages 90 à 92	https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf	Section du cadre de divulgation illustratif de la PPSAI détaillant la réponse minimale requise

Mise en œuvre connexe de l'étape 1 de l'EPDP *:*
Recommandation 18 :

- Exigences relatives à l'information devant figurer dans les réponses. Lorsque la divulgation des données (en tout ou en partie) a été refusée, une réponse devrait comprendre : des justifications suffisantes pour permettre au requérant de comprendre les raisons du refus, y compris, par exemple, une analyse et une explication de la façon dont le test d'équilibre de la requête a été effectué (le cas échéant).
- Les registres des demandes, des accusés de réception et des réponses devraient être conservés conformément aux pratiques commerciales standard en matière d'archivage, afin que ces pièces puissent être produites selon les besoins, y compris, mais sans s'y limiter, par l'équipe de la conformité de l'ICANN à des fins d'audit ;
- Le délai de réponse au requérant n'accusera aucun retard injustifié et, sauf circonstances exceptionnelles, ne dépassera pas les 30 jours. Ces circonstances peuvent comprendre le nombre total de requêtes reçues. Les parties contractantes informeront régulièrement le nombre de demandes reçues à l'ICANN afin de pouvoir évaluer si le délai est raisonnable.
- Pour la réponse aux requêtes de divulgation raisonnables à caractère « urgent », autrement dit les requêtes pour lesquelles une preuve est avancée étayant la nécessité d'une divulgation immédiate, un délai distinct de [moins de X jours ouvrables] sera considéré [le délai pour les demandes urgentes ainsi que les critères y associés seront définis pendant la mise en œuvre].

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : Août

i) Politiques acceptables en matière d'utilisation

Objectif : Définir les exigences en matière de politique concernant :

1. Comment un code de conduite (le cas échéant) devrait-il être élaboré, évoluer en permanence et être appliqué ?
2. Si l'ICANN et ses parties contractantes élaborent un code de conduite pour des tiers ayant un intérêt légitime, quelles caractéristiques et quels besoins devraient être pris en compte ?
3. Y a-t-il des flux de données supplémentaires qui doivent être documentés en dehors de ce qui a été documenté dans le cadre de l'étape 1 ?

Un modèle de code de conduite peut-il être un compliment ou être utilisé avec ce qui est mis en œuvre dans le cadre de la Recommandation 18 de l'étape 1 de l'EPDP ?

Questions connexes de la carte heuristique :

P1-Charter-c
c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?
c2) Quelles règles/politiques régiront l'utilisation des données par les utilisateurs une fois qu'ils y auront accédé ?
c3) Qui sera responsable de l'établissement et de l'application de ces règles/politiques ?
c4) Le cas échéant, à quelles sanctions ou pénalités un utilisateur devra-t-il répondre pour l'utilisation malveillante des données, y compris les futures restrictions à l'accès ou la compensation aux personnes concernées dont les données ont été utilisées à des fins malveillantes au-delà des sanctions déjà prévues par la loi applicable ?
c5) Les parties contractantes seront-elles au courant des données auxquelles on accède et sur la façon dont elles sont utilisées ?
c6) Les personnes concernées ont-elles le droit de savoir quand et comment leurs données sont consultées et utilisées ?
c7) Comment un modèle d'accès tiers peut-il tenir compte des différentes exigences relatives à la notification des personnes concernées vis-à-vis de la divulgation de leurs données ?

Documents à examiner :

Description	Lien	Fondements du caractère obligatoire
Article 40 du RGPD, Code de conduite	https://gdpr-info.eu/art-40-gdpr/	
Lettre du groupe de travail Article 29 à l'ICANN 11 avril 2018	https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf	
Bird & Bird - Code de conduite et documentation de référence sur la certification (mai 2017)	https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/43--guide-to-the-gdpr--codes-of-conduct-and-certifications.pdf?la=en	
Exemple : Code de conduite des fournisseurs de services de nuage (CISPE) (janvier 2017)	https://cispe.cloud/code-of-conduct/	
Exemple : Code de conduite des fournisseurs de services de nuage (EU Cloud) (novembre 2018)	https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html	

Mise en œuvre connexe de l'étape 1 de l'EPDP : Aucune.

Tâches :

- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : Août

j) Conditions d'utilisation / accords de divulgation / politiques de confidentialité

Objectif : Définir les exigences de politique concernant les conditions d'utilisation pour les tiers qui cherchent à accéder aux données d'enregistrement non publiques :

- au minimum, quelles sont les mesures nécessaires pour protéger de manière adéquate les données à caractère personnel qui peuvent être mises à la disposition d'un utilisateur ou d'un tiers accrédité ?
- quelles procédures devraient être établies pour accéder aux données ?
- quelles procédures devraient être établies pour limiter l'utilisation des données auxquels l'accès est correctement accordé ?
- des conditions d'utilisation distinctes devraient-elles être requises pour les différents groupes d'utilisateurs ?
- qui surveillerait et ferait respecter les conditions d'utilisation ?
- quel mécanisme serait utilisé pour exiger le respect des conditions d'utilisation ?

Questions connexes de la carte heuristique :

P1-Charter-c
c1) Quelles règles/politiques régiront l'accès des utilisateurs aux données ?
c2) Quelles règles/politiques régiront l'utilisation des données par les utilisateurs une fois qu'ils y auront accédé ?
c3) Qui sera responsable de l'établissement et de l'application de ces règles/politiques ?
c4) Le cas échéant, à quelles sanctions ou pénalités un utilisateur devra-t-il répondre pour l'utilisation malveillante des données, y compris les futures restrictions à l'accès ou la compensation aux personnes concernées dont les données ont été utilisées à des fins malveillantes au-delà des sanctions déjà prévues par la loi applicable ?

TSG-Final-Q#4
Indiquer si tous les requérants en général ou seule une catégorie particulière de requérants peut télécharger les journaux de leur activité.
TSG-Final-Q#10
Décrire les conditions, le cas échéant, dans lesquelles les demandes seraient divulguées aux parties contractantes.
TSG-Final-Q#11
Fourniture d'une analyse juridique concernant la responsabilité des opérateurs des différentes composantes du système.
TSG-Final-Q#12

Décrire une procédure de règlement des plaintes concernant des divulgations inappropriées et, par conséquent, d'une politique d'utilisation acceptable

Documents à examiner :

Description	Lien	Fondements du caractère obligatoire
Cadre préliminaire pour un éventuel modèle d'accès unifié pour l'accès continu à l'intégrale des Données WHOIS - Quel serait le rôle des conditions d'utilisation dans un modèle d'accès unifié ?	https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf pages 14 à 16	

Mise en œuvre connexe de l'étape 1 de l'EPDP :

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : septembre

k) Conservation et destruction des données

Objectif : Établir des exigences minimales en matière de politique pour la conservation, la suppression et la journalisation des données conservées pour les parties impliquées au SSAD, y compris, mais limité à, les données d'enregistrement de gTLD, les informations de compte d'utilisateur, les journaux des transactions et les métadonnées telles que la date et l'heure des requêtes

Questions connexes de la carte heuristique :

P1-Charter-c

c2) Quelles règles/politiques régiront l'utilisation des données par les utilisateurs une fois qu'ils y auront accédé ?

TSG-Final-Q#5
Description des exigences de conservation des données imposées à chaque composant du système.

Documents à examiner :

Description	**Lien**	**Fondements du caractère obligatoire**
Article 5(1)(e) du RGPD	https://gdpr.algolia.com/gdpr-article-5	
Conservation des données dans le modèle du TSG	https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf page 26	

Mise en œuvre connexe de l'étape 1 de l'EPDP : Recommandation 15 :
1. Afin d'éclairer ses délibérations de l'étape 2, l'équipe responsable de l'EPDP recommande que l'organisation ICANN entreprenne d'urgence une révision de tous ses processus et procédures en vigueur afin de recenser et de documenter les cas dans lesquels des données à caractère personnel sont requises à un bureau d'enregistrement au-delà de la période de « durée de l'enregistrement ». Les périodes de conservation de certains éléments de données devraient alors être définies, documentées et prises en compte pour établir les attentes minimales pertinentes et spécifiques requises concernant la conservation des données par les bureaux d'enregistrement. L'équipe responsable de l'EPDP recommande que les membres de la communauté soient invités à participer à cet exercice de collecte de données en formulant des commentaires sur d'autres finalités légitimes pour lesquelles des périodes de conservation différentes seraient applicables.

2. Dans l'intervalle, l'équipe responsable de l'EPDP a constaté que la politique de règlement de litiges relatifs au transfert (« TDRP ») a été identifiée comme ayant la plus longue période de conservation justifiée, à savoir un an, et a donc recommandé que les bureaux d'enregistrement soient tenus de ne conserver que les éléments de données jugés nécessaires aux fins de la TDRP, et cela pour une période de 15 mois après la fin de l'enregistrement, plus trois mois pour la mise en œuvre de la suppression, soit 18 mois au total. Cette conservation est fondée sur une disposition de la politique énoncée dans la TDRP qui prévoit que les plaintes présentées aux termes de la politique ne peuvent être déposées que pendant la période des 12 mois suivant la violation alléguée (FN : consulter l'article 2.2 de la TDRP) de la politique de transfert (FN : consulter l'article 1.15 de la TDRP). Ladite période de conservation ne limite pas la capacité des opérateurs de registre et des bureaux d'enregistrement à conserver pour des périodes plus courtes des éléments de données prévus dans les recommandations 4 à 7 à d'autres finalités précisées dans la Recommandation 1.

3. L'équipe responsable de l'EPDP reconnait que les parties contractantes pourraient avoir des besoins ou des exigences pour des périodes de conservation différentes conformes aux lois locales ou à d'autres exigences. L'équipe responsable de l'EPDP fait observer que rien dans cette recommandation ou dans toute autre politique distincte mandatée par l'ICANN n'interdit aux parties contractantes d'établir leurs propres périodes de conservation qui peuvent être plus longues ou plus courtes que ce qui est spécifié dans la politique de l'ICANN.

4. L'équipe responsable de l'EPDP recommande que l'organisation ICANN réexamine son processus actuel de dérogation à l'obligation de conservation de données dans le but d'améliorer l'efficacité, les délais de réponse aux demandes et la conformité au RGPD. Ainsi, si un bureau d'enregistrement d'une certaine juridiction a réussi à obtenir la dérogation à l'obligation de conservation de données, d'autres bureaux se trouvant dans une situation analogue pourront demander la même dérogation à travers une procédure de notification, sans avoir à présenter une demande séparée.

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : septembre

l) Viabilité financière

Objectif : Garantir que tous les aspects du SSAD soient financièrement viables. Réfléchir à la manière d'assumer les coûts de la mise en œuvre et de la gestion du SSAD, et qui en sera responsable.

- Déterminer si les inefficacités du marché existaient avant mai 2018 et si elles subsistent après la mise en œuvre de l'étape 1 de l'EPDP.
- Les parties contractantes et/ou l'ICANN devraient-elles assumer le coût d'une solution normalisée, même si la divulgation des données d'enregistrement est considérée d'intérêt public ?
- Si l'accréditation est une solution viable, devrait-on associer des frais de demande ou une structure de frais devrait-elle être basée sur le type (à plusieurs niveaux), la taille ou la quantification des divulgations ?
- Les personnes concernées devraient-ils ou pourraient-ils être rémunérés pour la divulgation de leurs données ?

Questions connexes de la carte heuristique : Aucune

Documents à examiner :

Description	Lien	Fondements du caractère obligatoire

Mise en œuvre connexe de l'étape 1 de l'EPDP : Aucune

Tâches :

- Confirmer les définitions des termes clés
- Déterminer la liste complète des questions de politique et discuter de chacune
- Déterminer les solutions possibles ou les recommandations proposées, le cas échéant
- Confirmer que toutes les questions relatives à la charte aient été abordées et documentées

Date cible d'achèvement : à déterminer

Annexe B – Contexte général

Contexte thématique et du processus

Le 19 juillet 2018, le conseil de la GNSO a lancé un processus accéléré d'élaboration de politiques (EPDP) et a formé l'équipe de l'EPDP sur la spécification temporaire relative aux données d'enregistrement des gTLD. Contrairement à d'autres PDP de la GNSO qui sont ouverts à tous ceux qui souhaitent y prendre part, le conseil de la GNSO a décidé de limiter la composition de cet EPDP, essentiellement en vertu de la nécessité de finir le travail dans un délai relativement court et du besoin de gérer de manière responsable les ressources destinées à cet effort. Les groupes de représentants de la GNSO, le Comité consultatif gouvernemental (GAC), l'Organisation de soutien aux extensions génériques (ccNSO), le Comité consultatif At-Large (ALAC), le Comité consultatif sur la sécurité et la stabilité (SSAC) et le Comité consultatif du système des serveurs racine (RSSAC) ont été invités à désigner chacun un nombre limité de membres et de suppléants, tel que décrit dans la charte. En outre, l'organisation ICANN et son Conseil d'administration ont été invités à désigner un nombre limité d'agents de liaison pour participer à cette initiative. Un appel à volontaires a été adressé aux groupes susmentionnés en juillet, et l'équipe responsable de l'EPDP a tenu sa première réunion le 1er août 2018.

Contexte de la problématique

Le 17 mai 2018, le Conseil d'administration de l'ICANN a approuvé la Spécification temporaire relative aux données d'enregistrement des gTLD. Le Conseil d'administration l'a approuvée dans le but d'établir les dispositions temporaires qui régiront la manière dont l'ICANN et ses parties contractantes continueront à respecter les obligations contractuelles et les politiques en matière de WHOIS élaborées par la communauté, tout en se conformant au Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). La spécification temporaire a été adoptée en vertu de la procédure prévue pour les politiques temporaires, décrite dans le contrat de registre (RA) et le contrat d'accréditation de bureau d'enregistrement (RAA). À la suite de l'adoption de la Spécification temporaire, le Conseil d'administration « devra mettre en œuvre immédiatement le processus d'élaboration de politiques de consensus prévu dans les statuts de l'ICANN ».[47] Ce processus d'élaboration de politiques de consensus sur la Spécification temporaire devrait être achevé dans un délai d'un an. En outre, la portée du travail inclut des discussions sur un système normalisé d'accès aux données d'enregistrement non publiques.

[47] Consulter l'article 3.1(a) du Contrat de registre : https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en

Lors de sa réunion du 19 juillet 2018, le conseil de l'Organisation de soutien aux extensions génériques (GNSO) a lancé un EPDP sur la Spécification temporaire relative aux données d'enregistrement des gTLD et a adopté la charte de l'équipe responsable de l'EPDP. Contrairement à d'autres PDP de la GNSO qui sont ouverts à tous ceux qui souhaitent y prendre part, le conseil de la GNSO a décidé de limiter la composition de cet EPDP, essentiellement en vertu de la nécessité de finir le travail dans un délai relativement court et du besoin de gérer de manière responsable les ressources destinées à cet effort. Les groupes de représentants de la GNSO, le Comité consultatif gouvernemental (GAC), l'Organisation de soutien aux extensions génériques (ccNSO), le Comité consultatif At-Large (ALAC), le Comité consultatif sur la sécurité et la stabilité (SSAC) et le Comité consultatif du système des serveurs racine (RSSAC) ont été invités à désigner chacun un nombre limité de membres et de suppléants, tel que décrit dans la charte. En outre, l'organisation ICANN et son Conseil d'administration ont été invités à désigner un nombre limité d'agents de liaison pour participer à cette initiative.

Le 21 novembre 2018, cette équipe a publié le rapport initial de l'étape 1 pour consultation publique. L'équipe responsable de l'EPDP a incorporé les commentaires publics dans son rapport final de l'étape 1, et le conseil de la GNSO a adopté les 29 recommandations du rapport final de l'étape 1 de l'EPDP à travers le vote lors de sa réunion du 4 mars 2019. Le 15 mai 2019, le Conseil d'administration de l'ICANN a adopté le rapport final de l'étape 1 de l'équipe responsable de l'EPDP, à l'exception de certaines parties de deux recommandations : 1) la finalité 2 de la Recommandation 1, et 2) la possibilité de supprimer des données dans le champ « Organisation » de la Recommandation 12. Conformément aux statuts constitutifs de l'ICANN, une consultation aura lieu entre le conseil de la GNSO et le Conseil d'administration de l'ICANN pour discuter des parties des recommandations de l'étape 1 de l'EPDP qui n'ont pas été adoptées par le Conseil d'administration de l'ICANN. En même temps, une Équipe de révision de la mise en œuvre (IRT), composée par l'organisation ICANN (ICANN org) et par des membres de la communauté de l'ICANN, mettra maintenant en œuvre les recommandations approuvées du rapport final de l'étape 1 de l'équipe responsable de l'EPDP. Pour de plus amples détails sur l'état de la mise en œuvre, veuillez consulter ici.

Le 2 mai 2019, l'équipe responsable de l'EPDP a lancé l'étape 2 de ses travaux. La portée de l'étape 2 de l'EPDP comprend : (i) la discussion sur un système normalisé d'accès et de divulgation des données d'enregistrement non-publiques, (ii) les questions citées dans l'annexe de la Spécification temporaire relative aux données d'enregistrement des gTLD (« Questions importantes nécessitant des mesures de la part de la communauté »), et (iii) les questions en suspens reportées de l'étape 1, p. ex., la distinction entre personnes physiques et personnes morales, l'expurgation du champ « ville », etc. Pour de plus amples renseignements, veuillez consulter ici.

ANNEXE C – Adhésion et participation à l'équipe responsable de l'EPDP

Adhésion et participation à l'équipe responsable de l'EPDP

Résumé des activités de la réunion :

Séances plénières :

- 75 appels pléniers, soit 155,5 heures
- 12 réunions en personne, soit 77,5 heures
- 01 séminaire en ligne, soit 1,0 heure
- Taux de participation total de 86 %

Réunions en petites équipes :

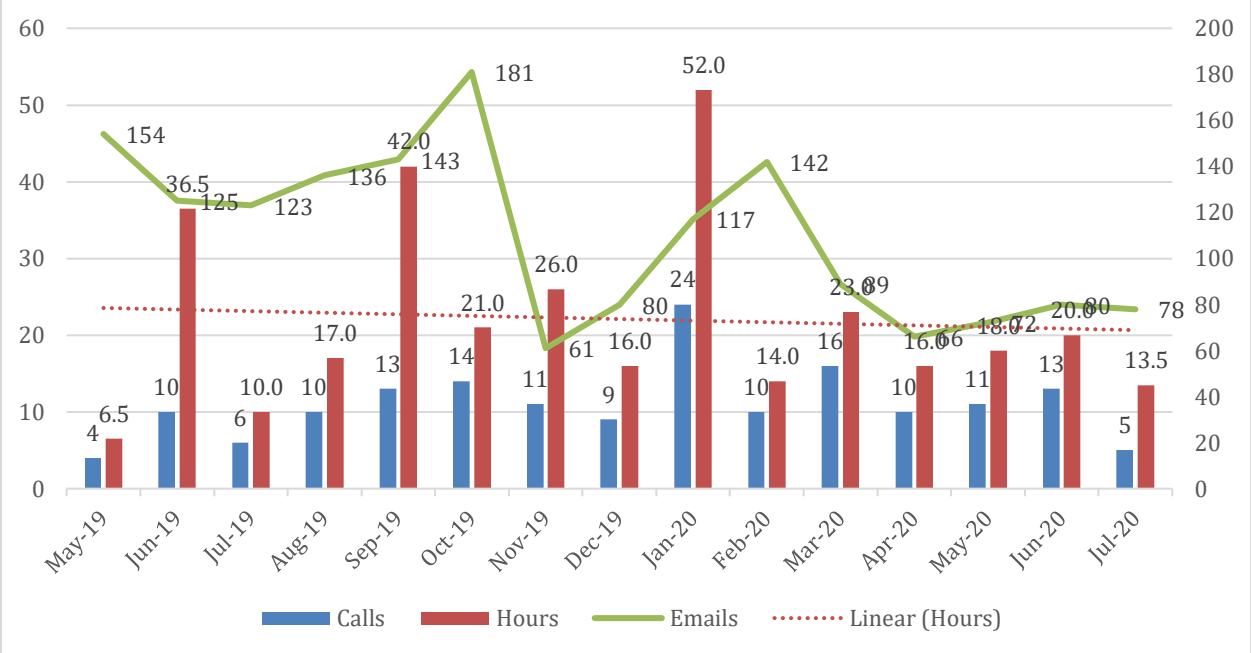
- 10 appels des sous-groupes, soit 18,0 heures

Réunions du Comité juridique :

- 19 appels des sous-groupes, soit 29,4 heures
- 01 réunions en personne, soit 1,5 heures

Réunions de l'équipe de direction :

- 48 appels des dirigeants, soit 47,5 heures
- 04 réunions des dirigeants en personne, soit 20,5 heures



Les registres de présence, les manifestations d'intérêt et autres sont disponibles sur : https://community.icann.org/x/kBdIBg.

Les archives contenant les courriers électroniques peuvent être consultées sur http://mm.icann.org/pipermail/gnso-epdp-team/.

Membres actifs de la plénière de l'équipe responsable de l'EPDP : (LC – membre du Comité juridique)

Type de membre / Affiliation / Nom	SOI	Date de début	% de participation	Rôle
Participant actuel			87,9 %	
Membre				
Comité consultatif At-Large			97,7 %	
Alan Greenberg	SOI	03/04/2019	97,7 %	
Hadia El Miniawi	SOI	03/04/2019	97,7 %	LC
Unité constitutive des entreprises et des utilisateurs commerciaux			94,8 %	
Margie Milam	SOI	03/04/2019	95,4 %	LC
Mark Svancarek	SOI	03/04/2019	94,3 %	
Conseil de la GNSO			98,3 %	
Rafik Dammak	SOI	03/04/2019	98,3 %	Président
Comité consultatif gouvernemental			93,6 %	
Christopher Lewis-Evans	SOI	15/05/2019	96,6%	
Georgios Tselentis	SOI	03/04/2019	88,5%	
Laureen Kapin	SOI	21/10/2019	96,1 %	LC
Conseil d'administration de l'ICANN			84,6 %	
Becky Burr	SOI	09/09/2019	93,5 %	LC
Chris Disspain	SOI	03/04/2019	78,2 %	
Unité constitutive des représentants de la propriété intellectuelle			91,0 %	
Brian King	SOI	04/08/2019	88,5 %	LC
Franck Journoud	SOI	12/01/2019	95,7 %	
Société pour l'attribution des noms de domaine et des numéros sur Internet			95,9 %	
Daniel Halloran	-	03/04/2019	94,3 %	
Eleeza Agopian	-	06/12/2019	98,4 %	
Unité constitutive des fournisseurs de services Internet et de services de connectivité			65,5 %	
Fiona Asonga	SOI	03/04/2019	44,8 %	
Thomas Rickert	SOI	03/04/2019	86,2 %	LC
Groupe des représentants des entités non commerciales			78,9 %	
Amr Elsadr	SOI	03/04/2019	67,8 %	
Johan (Julf) Helsingius	SOI	03/04/2019	75,9 %	
Milton Mueller	SOI	03/04/2019	81,4 %	
Stefan Filipovic	SOI	21/05/2019	84,5 %	

Stephanie Perrin	SOI	03/04/2019	86,2 %	LC
<vacant>	-			
Groupe des représentants des bureaux d'enregistrement			85,0 %	
James Bladel	SOI	03/04/2019	76,7 %	
Matt Serlin	SOI	03/04/2019	86,2 %	
Volker Greimann	SOI	16/04/2019	92,0 %	LC
Groupe des représentants des opérateurs de registre			90,0 %	
Alan Woods	SOI	03/04/2019	90,8 %	
Marc Anderson	SOI	03/04/2019	95,4 %	
Matthew Crossman	SOI	03/04/2019	83,1 %	LC
Comité consultatif sur la sécurité et la stabilité			92,1 %	
Ben Butler	SOI	03/04/2019	93,1 %	
Tara Whalen	SOI	15/05/2019	90,9 %	LC

Suppléants actifs de la plénière de l'équipe responsable de l'EPDP :

Type de membre / Affiliation / Nom	SOI	Date de début	% de participation	Rôle
Suppléant				
Comité consultatif At-Large				
Bastiaan Goslings	SOI	03/04/2019	50,0 %	
Holly Raiche	SOI	03/04/2019	33,3 %	
Unité constitutive des entreprises et des utilisateurs commerciaux				
Steve DelBianco	SOI	03/04/2019	100,0 %	
Comité consultatif gouvernemental				
Olga Cavalli	SOI	22/05/2019	95,6 %	
Rahul Gosain	SOI	03/04/2019	75,0 %	
Ryan Carroll	SOI	18/12/2019	100,0 %	
Unité constitutive des fournisseurs de services Internet et de services de connectivité				
Suman Lal Pradhan	SOI	03/04/2019	33,3 %	
Groupe des représentants des entités non commerciales				
David Cake	SOI	03/04/2019	90,0 %	
Tatiana Tropina	SOI	03/04/2019	77,8 %	LC
Yawri Carr Quirós	SOI	17/02/2020	100,0 %	
Groupe des représentants des bureaux d'enregistrement				
Owen Smigelski	SOI	16/04/2019	100 %	
Sarah Wyld	SOI	03/04/2019	98,7 %	
Theo Geurts	SOI	03/04/2019	80,0 %	
Groupe des représentants des opérateurs de registre				
Arnaud Wittersheim	SOI	03/04/2019	80,0 %	
Beth Bacon	SOI	22/04/2019	95,7 %	
Sean Baseri	SOI	06/11/2019	100,0 %	

Comité consultatif sur la sécurité et la stabilité				
Greg Aaron	SOI	05/10/2019	77,8 %	
Rod Rasmussen	SOI	03/04/2019	25,0 %	

Personnel de soutien actif auprès de la plénière de l'équipe responsable de l'EPDP :

Type de membre / Affiliation / Nom	SOI	Date de début	% de participation	Rôle
Soutien au personnel				
ICANN - Société pour l'attribution des noms de domaine et des numéros sur Internet				
Caitlin Tubergen		03/04/2019		LC
Marika Konings		03/04/2019		
Berry Cobb		03/04/2019		LC
Amy Bivens		03/06/2019		LC
Terri Agnew		03/04/2019		
Andrea Glandon		03/04/2019		
Julie Bisland		20/06/2019		
Michelle DeSmyter		20/06/2019		
Nathalie Peregrine		03/04/2019		

Anciens participants de la plénière de l'équipe responsable de l'EPDP :

Type de membre / Affiliation / Nom	SOI	Date de début	% de participation	Rôle	Date de départ
Ancien participant	-				
Membre	-				
Conseil de la GNSO	-				
Janis Karklins	SOI	03/04/2019	97,6%	Président	03/06/2020
Comité consultatif gouvernemental	-				
Ashley Heineman	SOI	03/04/2019	75,7%		21/10/2019
Conseil d'administration de l'ICANN	-				
Leon Felipe Sanchez Ambia	SOI	03/04/2019	88,5%	LC	09/09/2019
Unité constitutive des représentants de la propriété intellectuelle	-				
Alex Deacon	SOI	03/04/2019	87,5%		01/12/2019
Société pour l'attribution des noms de domaine et des numéros sur Internet	-				
Trang Nguyen	-	03/04/2019	88,9%	LC	10/04/2019
Groupe des représentants des entités non commerciales	-				
Ayden Fabien Férdeline	SOI	03/04/2019	73,5%		27/01/2020
Farzaneh Badiei	SOI	03/04/2019	69,2%		27/01/2020
Groupe des représentants des opérateurs de registre	-				
Kristina Rosette	SOI	22/04/2019	97,6%		07/08/2019
Suppléant	-				
Unité constitutive des représentants de la propriété intellectuelle	-				
Jennifer Gore	SOI	03/04/2019	97,6%		13/02/2020

Les registres de présence peuvent être consultés en détail sur https://community.icann.org/x/4opHBQ.

Les archives contenant les courriers électroniques peuvent être consultées sur https://mm.icann.org/pipermail/gnso-epdp-team/.

Annexe D - Désignation des consensus

Ci-dessous figure la désignation du président concernant le niveau de consensus pour chacune des recommandations du rapport final de l'équipe responsable de l'EPDP. Ces désignations ont été attribuées en suivant le processus décrit ici et conformément à la section 3.6 - Méthodologie standard pour la prise de décision des directives de la GNSO pour les groupes de travail et de la charte de l'équipe responsable de l'EPDP.

Recommandation	Désignation proposée par le président	Groupes n'appuyant pas la recommandation ou une partie de celle-ci
1 Accréditation	Consensus complet	
2 Accréditation des entités gouvernementales	Consensus complet	
3 Critères et contenu des requêtes	Consensus complet	
4 Accusé de réception	Consensus complet	
5 Exigences de réponse	Fort soutien mais opposition significative	GAC (exactitude) IPC BC
6 Niveaux de priorité	Divergence	GAC (n'appuie pas la 6.2) BC (n'appuie pas la 6.2) IPC (n'appuie pas la 6.2) ALAC (n'appuie pas la 6.2) SSAC
7 Finalités du requérant	Consensus	NCSG (sous réserve de la suppression de la note en bas de page)
8 Autorisation de la partie contractante	Fort soutien mais opposition significative	GAC (exactitude et objection à la 8.17) IPC BC
9 Automatisation du traitement SSAD	Fort soutien mais opposition significative	IPC BC ALAC
10 Détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD	Fort soutien mais opposition significative	RrSG (n'appuie pas les SLA pour les requêtes urgentes) SSAC IPC BC

11 Conditions générales du SSAD	Consensus complet	
12 Demandes de divulgation	Fort soutien mais opposition significative	GAC (exactitude) SSAC
13 Politique régissant les requêtes	Consensus complet	
14 Durabilité financière	Divergence	ALAC GAC SSAC IPC BC
15 Tenue de registres	Consensus complet	
16 Audits	Consensus complet	
17 Exigences en matière de rapports	Consensus complet	
18 Examen de la mise en œuvre des recommandations de politiques portant sur le SSAD par un comité permanent de la GNSO	Fort soutien mais opposition significative	ALAC BC IPC GAC
19 Affichage des informations des fournisseurs affiliés de services d'anonymisation et d'enregistrement fiduciaire	Consensus complet	
20 Champ « ville »	Consensus	NCSG
21 Conservation des données	Consensus complet	
22 Finalité 2	Consensus	NCSG

Annexe E - Déclarations minoritaires

Comité consultatif At-Large (ALAC)
Unité constitutive des utilisateurs commerciaux (BC)/Unité constitutive des représentants de la propriété intellectuelle (IPC)
Comité consultatif gouvernemental (GAC)
Groupe des représentants des entités non commerciales (NCSG)
Groupe des représentants des bureaux d'enregistrement (RrSG)
Groupe des représentants des opérateurs de registre (RySG)
Comité consultatif sur la sécurité et la stabilité (SSAC)

EN

AL-ALAC-ST-0720-04-01-EN
TEXTE ORIGINAL : Anglais
DATE : 29 juillet 2020
STATUT : Ratifié

COMITÉ CONSULTATIF AT-LARGE

Déclaration de l'ALAC portant sur le processus accéléré d'élaboration de politiques (EPDP)

Déclaration de l'ALAC pour inclusion dans le rapport final de l'étape 2 du processus accéléré d'élaboration de politiques (EPDP) consacré à la spécification temporaire relative aux données d'enregistrement des gTLD

L'ALAC a initié l'EPDP en faisant la déclaration suivante :

1. L'ALAC considère que l'EPDP DOIT porter ses fruits et œuvrera en ce sens.
2. Nous sommes en train de mettre sur pied une structure de soutien pour nous assurer que ce que nous présentons puisse être correctement compris par la communauté et dans le but de recevoir ses contributions et son appui.
3. L'ALAC considère que les titulaires de noms de domaine font partie des utilisateurs et œuvre régulièrement en leur nom (comme dans le cas du PDP lancé pour protéger leurs droits lorsque leurs domaines expirent) ; toutefois, dans les situations où leurs besoins ne s'accordent pas avec ceux des 4 milliards d'utilisateurs de l'Internet non titulaires de noms de domaine, ces derniers doivent prévaloir. Tel est le cas pour le RGPD et son EPDP.
4. Bien que certains utilisateurs qui consultent le WHOIS ne seront plus à même de le faire dans certaines situations à l'avenir, notre préoccupation principale vise à garantir l'accès aux tierces parties qui travaillent pour s'assurer que l'Internet reste un espace de sécurité pour ses utilisateurs, ce qui implique de laisser travailler en limitant au minimum l'accès aux données WHOIS des forces de l'ordre, des chercheurs en matière de cybersécurité, de ceux qui luttent contre la fraude au niveau des noms de domaines, de ceux qui aident à protéger les utilisateurs contre l'hameçonnage, les logiciels malveillants, le spam, la fraude et les attaques de déni de service distribué (DDoS). Toujours dans le respect, cela va de soi, des limites établies par le RGPD.

Nous avons travaillé sans relâche pour soutenir le processus accéléré d'élaboration de politiques et nous l'avons fait au nom des près de 5 milliards d'utilisateurs de l'Internet.

L'étape 2 de l'EPDP visait à développer ce qui s'appelle à présent Système normalisé d'accès et de divulgation aux données d'enregistrement non publiques (SSAD) ainsi qu'à répondre à certaines questions laissées en suspens lors de l'étape 1 de l'EPDP.

Bien que beaucoup d'efforts aient été réalisés, l'ALAC considère que lorsque le SSAD sera déployé, les chances qu'il réponde aux attentes des communautés dont nous soutenons les efforts seront faibles. Ces communautés doivent avoir accès à des données non-publiques, utiles et fiables de façon opportune et prévisible.

Pour y parvenir, la méthodologie à suivre implique de :

- Ne pas élargir la portée des législations en matière de protection de la vie privée. N'expurger que les données protégées par ces lois.
- S'assurer de la fiabilité des données et de la possibilité d'utiliser les informations de contact - ce qui est leur seule raison d'être.
- Dans la mesure du possible et de la légalité, traiter les requêtes de façon automatique afin de fournir des réponses rapides (voire quasi instantanées lorsque cela s'avère possible).

Malheureusement, le rapport final ne suit aucun de ces postulats.

Plus particulièrement :

- L'étape 1 autorise l'expurgation d'informations concernant aussi bien des personnes morales (entreprises) que physiques (individus), la plupart des bureaux d'enregistrement et des opérateurs de registre se livrant à ces expurgations complètes. Ils le font indépendamment des localisations géographiques.
- L'étape 2 était censée aborder la distinction entre personnes morales et physiques, mais, malgré les débats, la question fut renvoyée au conseil de la GNSO pour qu'il se prononce sur ce sujet ultérieurement.
- Au titre du RGPD, les données doivent être exactes pour le but dans lequel elles sont traitées. Dans le cas des données RDS, cela implique de savoir qui est le titulaire du nom de domaine et de faciliter le contact. Les études portant sur l'exactitude du WHOIS montrent que lorsque l'information est accessible au public, celle-ci tend à être fâcheusement inexacte. L'étape 2 devait traiter en profondeur du thème de l'exactitude des données en lien avec les données à présent expurgées. Cela n'a pas été fait. Le PDP a reçu pour consigne du conseil de la GNSO de ne pas aborder ce thème que ce dernier traitera ultérieurement sous une forme non encore spécifiée.

- Actuellement le contact avec les titulaires de noms de domaine se fait à travers des méthodes (essentiellement des formulaires en ligne) dont les études ont démontré l'absence d'efficacité, l'expéditeur n'ayant pas moyen de savoir si le message est parvenu au titulaire du nom de domaine. Les discussions sur ce thème sont renvoyées au conseil de la GNSO pour qu'il y réponde ultérieurement.
- Pour certains cas d'utilisation, le SSAD envoie une réponse automatique. L'intention était que, à mesure que la loi, la jurisprudence et les aspects contractuels progressent, il soit possible de gérer davantage de cas d'utilisation de forme automatique à travers un mécanisme « évolutif ». Le mécanisme évolutif recommandé consiste en un comité permanent de la GNSO en charge de faire approuver tous les nouveaux cas d'utilisation non seulement par les parties contractantes (passibles de pénalités si elles ne le font pas correctement), mais également par le conseil de la GNSO. Le comité permanent peut émettre des recommandations de mise en œuvre (exigeant l'accord du conseil de la GNSO pour y procéder) et de politique (impliquant préalablement un processus d'élaboration de politiques de la GNSO tel qu'un PDP). Il reste à savoir si les nouvelles recommandations à propos des décisions du SSAD en fonction des cas d'utilisation correspondent à la mise en œuvre ou si, pour que le système puisse être automatisé, un tout nouveau PDP (ou équivalent) devrait être entrepris au préalable (retardant ainsi potentiellement de plusieurs années l'application de nouveaux cas d'utilisation).

  Malgré ses réserves, l'ALAC, comme d'autres groupes, a accepté le modèle actuel du SSAD, ayant reçu l'assurance que le mécanisme d'évolution permettrait d'apporter des modifications de façon pratique et opportune. Pour des questions juridiques et de responsabilité, de telles modifications ne pouvaient être garanties, mais restaient néanmoins possibles. Au vu de ce que nous savons à présent sur le mécanisme d'évolution, et le manque de clarté vis-à-vis de son fonctionnement et de la façon dont les recommandations seront traitées par le conseil de la GNSO, il est clair que l'ALAC n'aurait jamais approuvé le modèle actuel du SSAD.

  En outre, bien qu'une recommandation émanant du Comité permanent requière, par défaut, un vote majoritaire ordinaire du conseil de la

GNSO, rien n'empêche de modifier cela pour exiger dorénavant un vote à la majorité qualifiée[48].

- Le modèle financier est préoccupant. À première vue, bien que le fait de demander aux utilisateurs du SSAD d'assumer une partie significative des coûts d'exploitation puisse se justifier, le fait de fixer les prix en ce sens risque d'aboutir à des montants si élevés que cela décourage finalement d'utiliser le système. Ce qui reviendrait non seulement à ne pas atteindre les objectifs financiers fixés mais rendrait également vain l'ensemble de la démarche. La détermination des prix doit se faire de façon flexible pour que le SSAD puisse véritablement être utilisé. En ce sens, il n'est pas encore possible de savoir à quelle hauteur l'ICANN devra subventionner ce service.

Toutes ces difficultés tiennent au fait que l'EPDP a reçu pour instruction de ne pas se pencher sur cette question, ou qu'il a opté pour ne pas le faire ou encore formulé des recommandations en la matière suffisamment vagues dont il n'est pas possible d'estimer en toute confiance les résultats.

Toutes ces questions POURRAIENT recevoir un traitement adéquat du conseil de la GNSO lors de ses délibérations sur le rapport final.

Par conséquent, l'ALAC soutient ce rapport SOUS RÉSERVE que le conseil de la GNSO spécifie les mesures ci-dessous.

Si ces résultats ne sont pas atteints, l'ALAC considère que ce rapport entraînera une mise en œuvre pluriannuelle aboutissant à un simple système de tickets extrêmement complexe et coûteux. De ce fait, nous n'accordons point notre soutien au rapport final, à l'exception des Recommandations 9 à 22, que nous appuyons[49].

Les résultats du conseil de la GNSO requièrent que l'ALAC soutienne le rapport final de l'EPDP :

1. Le conseil de la GNSO reconnaît que toute recommandation émanant du comité permanent sur l'évolution portant sur le cas d'autres utilisations supplémentaires de décisions du SSAD (conformément à la recommandation de politique de l'EPDP 9.3) sera considérée comme une mise en œuvre et n'exigera pas de délibérations politiques supplémentaires.
2. Les questions portant sur la personnalité morale vs la personnalité physique, l'exactitude, le système de signalement de problèmes liés à

[48]Un vote à la majorité qualifiée permet à un groupe de parties prenantes accompagné d'un autre membre de la Chambre d'opposer son véto à toute action de la GNSO.

[49] Afin d'éviter toute confusion, si les conditions ne se retrouvent pas remplies, l'ALAC soutiendra quoiqu'il en soit les Recommandations 19 à 22 sans pour autant donner son soutien au reste du rapport.

l'exactitude du WHOIS et les contacts e-mail anonymisés seront entièrement traitées avec la pleine participation des comités consultatifs de l'ICANN souhaitant y participer, pour tous les aspects de la discussion. Si ces questions sont réputées comme étant des politiques, elles devront être abordées par un groupe mandaté pour élaborer des recommandations de politique et sous la direction d'un président qualifié et sans conflit d'intérêts. Le GAC, l'ALAC et le SSAC doivent être impliqués dans l'élaboration du mandat ou de la charte de ces groupes. La date butoir pour l'achèvement de tous les travaux ne devra pas excéder le mois d'avril de 2021.

3. Le Conseil de la GNSO reconnaît que la ratification des recommandations du Comité permanent sur l'évolution n'exige que la majorité de la GNSO tel que cela figure dans le manuel politique de la GNSO.
4. Le conseil de la GNSO reconnaît que les délibérations concernant la détermination des prix pour la mise en œuvre du SSAD ne doivent pas s'axer uniquement sur la récupération des coûts mais prendre en compte les utilisateurs potentiels du SSAD et leur capacité et volonté à payer les prix définis.

Approuvé à l'unanimité par l'ALAC, 29 juillet 2020
Présenté par Alan Greenberg au nom de l'ALAC

Supplément à la déclaration minoritaire de l'ALAC portant sur le rapport final de l'étape 2 de l'EPDP

Les membres du Comité consultatif At-Large (ALAC) apprécient cette opportunité de présenter leur supplément à la déclaration présentée le 29 juillet 2020.

L'ALAC et son équipe responsable du suivi de l'EPDP ont eu l'occasion d'examiner et de discuter des déclarations présentées par le BC/IPC, le GAC et le SSAC ainsi que celles présentées par les autres groupes membres de l'EPDP.

Bien que l'ALAC, la BC, l'IPC, le GAC et le SSAC aient pris chacun des approches distinctes pour exprimer leurs positions concernant le rapport, l'ALAC est en accord général avec les déclarations du GAC, du SSAC et de la BC et l'IPC. Plus particulièrement, l'ALAC apprécie l'analyse profonde et avisée menée par le GAC, le SSAC, la BC et l'IPC.

L'ALAC a pleinement conscience de ce qu'implique contester les résultats d'un difficile débat qui s'est déroulé sur plus d'un an. Pour dire les choses clairement, malgré ce qui a pu être parfois insinué, nous n'avons jamais cherché à contester le processus pour la simple raison que « nous n'avons pas obtenu ce que nous voulions ». Si les problématiques essentielles au bon fonctionnement du SSAD n'avaient pas été abordées, le système obtenu n'aurait pu répondre aux besoins des utilisateurs du SSAD

et l'opportunité de corriger ces problèmes à l'avenir aurait été faible. Nous espérons que la GNSO et, le cas échéant, le Conseil d'administration prendront cela en considération pour les prochaines étapes du processus.

Ratifié par l'ALAC, 24 août 2020.

Déclaration minoritaire de l'Unité constitutive des utilisateurs commerciaux (BC) et de l'Unité constitutive des représentants de la propriété intellectuelle (IPC) portant sur le rapport final de l'étape 2 de l'EPDP

Le rapport final de l'étape 2 de l'EPDP ne parvient pas à fournir un système d'accès normalisé capable de répondre aux besoins des utilisateurs. Par conséquent, l'Unité constitutive des utilisateurs commerciaux (BC) et l'Unité constitutive des représentants de la propriété intellectuelle (IPC) s'y opposent.

Tel que cela figure dans notre déclaration sur le rapport final de l'étape 1 de l'EPDP, la BC et l'IPC sont de fervents défenseurs du modèle multipartite ascendant et basé sur le consensus de l'ICANN, comme en témoigne notre participation active et de bonne foi à l'EPDP. L'étape 2 de l'EPDP a été conçue pour créer un système normalisé ayant le double objectif de protéger les données à caractère personnel des titulaires de noms de domaine et d'offrir aux utilisateurs un accès opportun et prévisible aux données des titulaires de noms de domaine lorsque les utilisateurs doivent traiter ces informations en toute légalité pour des finalités légitimes. Le rapport final de l'étape 2 ayant manqué à ce but, nous ne pouvons l'accepter.

Inquiétudes manifestées

L'IPC et la BC défendent la protection de la vie privée pour les données à caractère personnel tout comme la loi en matière de vie privée vise à équilibrer le droit individuel à la vie privée et d'autres intérêts légitimes. Malheureusement, le rapport final de l'étape 2 n'est pas parvenu à cet équilibre. Cet échec représente un détriment pour ceux qui défendent leurs droits fondamentaux et ceux qui agissent dans l'intérêt public ou tout autre intérêt légitime. Les membres de la BC visent à promouvoir la confiance des utilisateurs vis-à-vis des communications et des interactions commerciales en ligne (tel que cela figure dans la directive NIS de l'UE, par exemple). Les membres de l'IPC cherchent à protéger les consommateurs de l'hameçonnage, des produits contrefaits dangereux et autres fraudes conformément à l'article 38 de la Charte des droits fondamentaux de l'UE et à défendre la propriété intellectuelle conformément à la section 2 de l'article 17 de cette Charte.

L'IPC et la BC remarquent que le rapport final de l'étape 2 ne permet pas de répondre aux nombreuses préoccupations avancées par la Commission Européenne et l'autorité de protection des données (APD) belge, de même que par les comités consultatifs de l'ICANN : le Comité consultatif gouvernemental (GAC) représentant l'application de la loi et les intérêts de la défense des consommateurs, le Comité consultatif At-Large (ALAC) représentant les intérêts des utilisateurs finaux de l'Internet, et le Comité consultatif sur la sécurité et la stabilité (SSAC) tenu de conseiller le Conseil d'administration de l'ICANN en matière de sécurité et d'intégrité des systèmes de nommage et d'allocation d'adresses Internet.

Préoccupations manifestées par la Commission européenne et l'autorité de protection des données belge (APD).

La Commission européenne [50] a exhorté l'*« ICANN et la communauté de développer un modèle d'accès unifié qui s'applique à tous les registres et bureaux d'enregistrement et offre une méthode opérationnelle, prévisible et stable pour l'accès aux données d'enregistrement des gTLD non publiques pour les utilisateurs ayant un intérêt légitime ou un autre fondement juridique tel que le stipule le règlement général sur la protection des données (RGPD) ».* La Commission européenne a déclaré qu'elle considérait cela « *vital et urgent* » et a exhorté l'ICANN à « *développer et mettre en œuvre un modèle d'accès opérationnel et pratique dans les plus brefs délais*... ». L'Autorité de protection des données belge, qui constitue l'autorité de supervision de l'ICANN étant donné que l'UE siège en Belgique, appelle de ses vœux un modèle qui soit « *meilleur, basé sur le bon sens du point de vue de la sécurité et des données* ».[51] Malheureusement, le rapport final de l'étape 2 n'a pas permis d'aboutir à une méthode d'accès et encore moins à une méthode pouvant être qualifiée d'« *opérationnelle, prévisible et stable* ». Au contraire, le rapport final de l'étape 2 se contente d'offrir un lieu centralisé pour déposer les requêtes. En ce sens, il ne répond pas à l'orientation de l'Autorité de protection des données belge qui préconise de remettre toute décision relative à la divulgation de données à la discrétion des plus de deux mille parties contractantes, lesquelles ne sont pas contraintes, au titre des politiques et des contrats de l'ICANN, de disposer de conseils juridiques, de délégués à la protection des données ou d'experts en matière de respect de la vie privée.

Préoccupations manifestées par la BC et l'IPC et partagées par le GAC

Nous partageons également les préoccupations du GAC face à l'échec de l'équipe responsable de l'EPDP à répondre aux questions concernant l'exactitude des données et la distinction entre personnes physiques et morales. Dans sa lettre adressée au conseil de la GNSO, datée du 22 juin, [52]le GAC signale que « *Ces points sont essentiels à l'intérêt public*. *Ayant échoué à offrir des réponses à ces questions, l'EPDP actuel risque d'aboutir à un système qui ne soit pas en mesure de garantir la sécurité publique. En outre, l'échec à traiter ces dossiers importants ne fait que soulever des doutes quant à la légitimité et l'efficacité du processus d'élaboration de politiques de la GNSO pour répondre à ces questions fondamentales pour les parties prenantes de la GNSO et pour l'intérêt public* ». Malheureusement, cette requête du GAC a été ignorée dans l'étape 2. Bien que le RGPD exige l'exactitude des données, le conseil de la GNSO l'a retirée du mandat des travaux de l'étape 2 de l'EPDP et le rapport final de l'étape 2 de l'EPDP

[50]Consulter : https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf
[51] Consulter : https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[52] Consulter : https://gac.icann.org/advice/correspondence/outgoing/GAC%20Chair%20letter%20to%20GNSO%20Council%20Chair%20-%20Next%20Steps%20on%20Key%20Policy%20Issues%20not%20Addressed%20in%20EPDP%20Phase%202.pdf

n'est pas parvenu à distinguer entre la personne physique et morale titulaire d'un nom de domaine.

Préoccupations manifestées par la BC et l'IPC et partagées par le SSAC et l'ALAC

Les commentaires du SSAC portant sur le rapport initial de l'étape 1 de l'EPDP (SSAC 111[53]) ont soulevé de nombreuses questions quant au fait que les recommandations « *sont loin d'être à la hauteur de ce que le SSAC considère nécessaire et possible afin de répondre aux questions en matière de sécurité et de stabilité dont l'ICANN a l'attribution* ». De même, dans [54] sa déclaration du 5 mai 2020 au sujet du supplément au rapport initial, l'ALAC a également exprimé ses préoccupations face à l'échec à répondre aux questions liées à la distinction entre la personne physique et morale titulaire d'un nom de domaine et à l'exactitude, parmi d'autres.

Échecs majeurs du rapport final de l'étape 2 de l'EPDP

En outre des préoccupations énoncées précédemment par le GAC, l'ALAC et le SSAC, la BC et l'IPC sont en désaccord avec les erreurs suivantes figurant dans le rapport sur l'étape 2.

- ***Absence de divulgation centralisée et insuffisance des mécanismes d'évolution.*** Après l'étape 1, nous attendions le déploiement d'une politique en faveur d'un processus de prise de décisions décentralisé. Les inefficacités et incohérences inhérentes à un processus de prise de décisions décentralisé sont claires : coûts plus élevés pour les parties contractantes, procédures de requête de divulgation plus lentes ainsi que davantage de risques de litiges entre les requérants et les divulgateurs, chaque partie contractante appliquant pour chaque requête un point de vue subjectif.

  Quoiqu'il en soit, pour parvenir à un compromis, nous avons bien voulu considérer (bien que n'acceptant pas) le *modèle hybride* proposé d'après lequel les décisions seront initialement manuelles et décentralisées, avant d'évoluer vers un processus centralisé et automatisé, fondé sur l'expérience accumulée lors de la mise en œuvre du SSAD et sur la clarté juridique pour l'interprétation des exigences du RGPD.

  Nous espérons qu'au fil du temps et avec les sauvegardes nécessaires, le système pourra fournir automatiquement les données des titulaires de noms de domaine demandées à des fins légitimes par des requérants accrédités suivant les fondements juridiques qui sont les leurs. Ainsi, des requérants accrédités disposant de preuves raisonnables concernant la vente de produits contrefaits ou des atteintes aux droits d'auteur, déclarées sous peine de parjure, devraient

[53] **Consulter :** https://www.icann.org/en/system/files/files/sac-111-en.pdf
[54] Consulter : https://atlarge.icann.org/advice_statements/13775

pouvoir compter rapidement sur les données des titulaires de noms de domaine concernés. Alors qu'un système clair, cohérent et évolutif permettrait de renforcer grandement la responsabilité et la confiance vis-à-vis du système des noms de domaine et de l'accès qu'il permet à ses données, le rapport final de l'étape 2 ne va pas en ce sens.

Le rapport de l'étape 2 ne permet pas à l'ICANN d'évoluer, comme sa nature l'exige, vers un processus de prise de décisions décentralisé. Au contraire, il laisse à la discrétion totale des parties contractantes d'interpréter individuellement leurs obligations au titre du RGPD et des contrats souscrits avec l'ICANN sans le moindre prérequis en matière de raisonnabilité, d'harmonisation ou d'autres sauvegardes. Il ne parvient pas, en outre, à fournir un mécanisme adéquat en vue d'une centralisation et automatisation futures. De ce fait, il reste prisonnier de processus de prise de décisions décentralisés inefficaces tel que celui aboutissant à des conventions de service excessivement longues dans le cas de requêtes urgentes portant sur des menaces pour les individus ou des infrastructures critiques. (Recommandations 9 et 18)

- ***Incapacité à distinguer entre personnes physiques et morales.*** En laissant à la discrétion des parties contractantes de distinguer entre personne morale et physique, le rapport de l'étape 2 échoue à apporter davantage de clarté quant à l'accès aux données de *personnes morales* titulaires de noms de domaine non couvertes par le RGPD. L'équipe responsable de l'EPDP a requis à Bird & Bird de lui fournir un conseil juridique externe pour ses orientations en matière des obligations au titre du RGPD afin de distinguer entre les personnes morales et les personnes physiques titulaires de noms de domaine. Toutefois, elle n'a pas tenu compte des objections sur ce point de l'IPC, de la BC, du GAC, du SSAC et de l'ALAC. L'expurgation massive et permanente des données de contact des personnes morales n'est pas requise par le RGPD[55], et elle porte atteinte à la confiance, à la responsabilité et à la transparence du DNS. À ce titre, elle représente une erreur inacceptable de la part de l'EPDP. (Recommandation 8).

- ***Incapacité à résoudre l'inexactitude des données.*** Le rapport de l'étape 2 n'apporte aucune solution à la question essentielle de l'inexactitude des données des titulaires de noms de domaine tel que cela avait été accordé dans l'étape 1 de l'EPDP et bien que nous disposions aujourd'hui d'outils permettant de vérifier l'exactitude de ces données. L'inexactitude des données WHOIS a été problématique depuis 20 ans. L'équipe responsable de l'EPDP n'a pas été en mesure de suivre le conseil légal qu'elle a pourtant sollicité pour l'interprétation

[55] Les commentaires soumis par l'Afnic au supplément de l'étape 2 soutiennent ce point de vue. « *Nous souhaiterions faire part de notre préoccupation face à l'approche qui consiste à ne pas distinguer l'enregistrement des personnes physiques de celui des personnes morales. Tel que cela a déjà été signalé par nombre d'observateurs, nous considérons qu'il s'agit d'une application excessive du RGPD. Bien que le RGPD ne protège pas les données des personnes morales, nous rappelons à l'ICANN la lettre du WP29, datée du 11 décembre 2017 ».*

de l'exigence d'exactitude des données au titre du RGPD. L'équipe responsable de l'EPDP a également échoué à suivre le conseil émanant de la Commission européenne qui confirmait pourtant que l'exactitude des données ne se limite pas aux intérêts de la personne concernée. Les données manifestement fausses ne sont pas protégées par les lois de protection de la vie privée et le maintien de la modification massive de données des titulaires de noms de domaine fausses ou fictives dans le DNS constitue un autre signe d'échec de l'EPDP et porte atteinte à la confiance, à la responsabilité et à la transparence du DNS. (Conclusion 2)

- ***Politiques d'application de la loi inadéquates.*** Le rapport sur l'étape 2 ne contient aucun mécanisme responsabilisant les parties contractantes de fournir des données en cas de requêtes légitimes. Tel que mentionné précédemment, le rapport sur l'étape 2 ne parvient à fournir ni une base objective ni une procédure cohérente, prévisible et évolutive permettant aux utilisateurs accrédités d'obtenir des données des titulaires de noms de domaine exactes lorsqu'il existe un fondement juridique et une raison légitime pour le faire et pour utiliser ces données, même lorsque celles-ci n'auraient pas dû être cachées d'emblée. Le rapport de l'étape 2 échoue ainsi à habiliter l'ICANN à faire appliquer les quelques recommandations qu'il préconise. Sans un mécanisme garantissant l'application des politiques de consensus, un SSAD décentralisé n'a que peu de valeur. Il est à regretter que ce rapport ne prenne en considération que l'application des exigences de procédure et ne permette pas au service de conformité de l'ICANN d'examiner les refus injustifiés qui sont opposés à des requêtes légitimes. C'est l'ensemble de la politique qui se voit ainsi lésé et perd en légitimité. (Recommandations 5 et 8)

En conséquence, le rapport de l'étape 2 recommande un système et des politiques qui ne permettent pas l'achèvement des objectifs affichés et accordés pour le SSAD, notamment en ce qui concerne les besoins des utilisateurs. Ce rapport de l'étape 2 ne parvient donc pas à garantir la confiance, la sécurité et la résilience du DNS.

Il est fondamental que lors de l'élaboration de cette politique, la communauté de l'ICANN soutienne les efforts permettant de lutter contre l'accroissement au niveau de l'utilisation malveillante des noms de domaine portant atteinte à la sécurité, la stabilité et la résilience du DNS et de l'écosystème de l'Internet dans son ensemble, notamment en ce qui a trait à la sécurité et à la sécurité de ses utilisateurs. Récemment, face à l'augmentation globale du trafic Internet dû à la COVID-19 et aux cyberattaques qui l'accompagnent, la partie contractante Neustar a déclaré : « *Bien que Neustar se soit attendu à une augmentation, ces attaques ont connu une augmentation remarquable ayant tiré parti de pratiquement tous les indicateurs mesurés. Nous avons observé une augmentation du nombre total d'attaques ainsi que de leur sévérité...* »[56] Neustar

[56] Consulter : https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

signale avoir *« atténué plus du double des attaques au premier trimestre 2020 qu'au premier trimestre 2019 », ainsi qu'« une augmentation des détournements du DNS, par le biais de ses configurations et en redirigeant l'utilisateur vers un site Internet identique en apparence qui contient des programmes malveillants dissimulés sous forme d'éléments utiles ».*

Désignations par consensus

L'IPC et la BC rappellent au conseil de la GNSO et au Conseil d'administration de l'ICANN que le rapport final de l'étape 2 de l'EPDP définit les politiques à suivre en vue d'un **système** unique (à savoir, le SSAD). Bien que l'appel à consensus soit fait au niveau de chacune des recommandations, celles-ci sont, par nature, interconnectées et interdépendantes en raison de leur impact et influence sur l'ensemble du SSAD. Par conséquent, le résultat de l'appel à consensus ne devrait pas porter sur chacune des recommandations mais sur l'ensemble du système.

Recommandation	
1 Accréditation	Soutient
2 Accréditation des entités gouvernementales	Soutient
3 Critère et contenu des requêtes	Soutient
4 Accusé de réception	Soutient
5 Exigences de réponse	Soutient
6 Niveaux de priorité	Soutient
7 Finalités du requérant	Soutient
8 Autorisation des parties contractantes	Soutient
9 Procédure d'automatisation du SSAD	Soutient
Détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD	Soutient
11 Conditions générales d'utilisation du SSAD	Soutient
12 Exigences de divulgation	Soutient
13 Politique en matière de requêtes de renseignements	Soutient
14 Durabilité financière	Soutient
15 Tenue de registre	Soutient
16 Audits	Soutient
17 Exigences en matière de rapports	Soutient
18 Examen de la mise en œuvre des recommandations de politiques portant sur le SSAD par un comité permanent de la GNSO	Soutient
19 Affichage des informations des fournisseurs affiliés de services d'anonymisation et d'enregistrement fiduciaire	Soutient
20 Champ « ville »	Soutient
21 Conservation des données	Soutient
22 Finalité 2	Soutient

De plus, l'IPC et la BC s'opposent au libellé des sections suivantes, hors recommandations :

- Sections 1.2 et 2.3 (description des « sujets non abordés »). Nous n'appuyons pas la description du résultat du débat au sujet de la distinction entre personnes morales et personnes physiques.
- Section 3.1 (description de la façon dont nous sommes arrivés à un modèle « hybride »). Notre acceptation pour passer à un modèle hybride était conditionné à la possibilité de déléguer progressivement les décisions centralisées au CGM par le biais d'un mécanisme évolutif.
- Conclusion - Exactitude (page 60).

Évaluation de l'utilité générale pour les requérants

Bien que l'équipe responsable du suivi de l'étape 2 de l'EPDP ait consacré beaucoup de temps et d'efforts à analyser la durabilité financière du SSAD, nous considérons qu'il est également important d'analyser les coûts et les bénéfices du point de vue de l'utilisateur (notamment les utilisateurs du système demandant la divulgation des données des titulaires de noms de domaine). Étant donné qu'en vertu de la politique de l'étape 2, il appartient aux requérants d'assumer la plupart, voire l'ensemble, des coûts opérationnels et d'entretien du SSAD, cela risque d'entraîner d'importants frais de requête et d'accréditation à leur charge.

Au-delà des coûts directs, la politique du SSAD telle qu'elle est actuellement définie aura un impact significatif sur les coûts traditionnellement liés aux données WHOIS. Ces coûts indirects sont liés aux aspects ci-dessous :

- **Réponse trop tardive :** En raison des défaillances décrites précédemment, le délai de réponse aux demandes de divulgation sera excessivement long et aura un impact sur l'efficacité des processus de gestion et d'enquête des manquements et des situations illicites.

- **Incomplétude :** La recherche dite « inverse » n'étant plus possible, il devient désormais plus difficile d'identifier tous les domaines associés à un évènement ou à une attaque.

- **Non-attribution :** La suppression des recherches inverses pèse sur la capacité à associer un titulaire de nom de domaine (acteur) à une activité malveillante ou criminelle dans un laps de temps utile (si jamais on y parvenait). Les requérants, notamment ceux qui sont les premiers défendeurs en cas de cyberattaques, vont devoir dépendre de facteurs de proximité sans bénéficier d'une marge de manœuvre leur permettant de déployer des contre-mesures ou atténuer les attaques.

- **Inexactitude :** Rien ne garantit l'exactitude des données qui seront fournies, de même qu'il n'existe aucune disposition permettant aux parties indépendantes

de mener des audits pour assurer l'exactitude des données d'enregistrement. Les requérants sont chargés d'assumer le coût des demandes de divulgation sans garantie aucune de la valeur de la réponse obtenue.

- **Absence de confinement :** L'incapacité à fournir une énumération complète et en temps voulu des domaines associés à une activité malveillante ou criminelle retarde les première mesures visant à atténuer les cyberattaques. Les attaques peuvent ainsi persister bien au-delà des objectifs d'atténuation historiquement fixés à entre 1 et 4 heures. Les SLA, telles qu'elles sont actuellement définies, ne suffisent pas à contrer les activités d'hameçonnage dont la durée s'évalue en heures plus qu'en journées, ni les attaques de logiciels malveillants qui infligent de lourds coûts et des pertes directs à ceux qui en sont victimes.
- **Imprévisibilité :** Un modèle de divulgation distribué et décentralisé entraînera un système d'accès et de divulgation imprévisible et aléatoire. Celui-ci entravera les efforts des requérants souhaitant la divulgation des multiples parties contractantes impliquées dans l'ensemble des domaines concernées par toute activité malveillante ou cyberattaque.

Nous avons toujours admis la nécessité de payer des frais d'accréditation pour l'utilisation du SSAD. Toutefois, l'intérêt et les bénéfices qu'offre le SSAD, tel qu'ils figurent dans le rapport final de l'étape 2, ne justifient pas les coûts d'utilisation (directs ou indirects) du SSAD.

Conclusion

Lors de l'adoption, en mai 2018, de la Spécification temporaire, le Conseil d'administration de l'ICANN a signalé que « *les actions du Conseil d'administration doivent avoir un impact immédiat sur la sécurité, la stabilité ou la résilience continue du DNS, celui-ci œuvrant au maximum pour le maintien du WHOIS le temps que la communauté parvienne à l'élaboration d'une politique de consensus* ».[57] Lors de la réunion ICANN66 à Montréal, en novembre 2019, le Conseil d'administration et le Président-directeur général de l'ICANN ont réaffirmé, dans le cadre du forum ouvert, l'importance d'un accès évolutif aux données des titulaires de noms de domaine pour garantir la sûreté et la sécurité de l'Internet et de ses utilisateurs. Plus de deux ans de travaux intenses de l'équipe responsable de l'EPDP se sont soldés par un statut quo : les éléments des données WHOIS nécessaires à l'identification des titulaires et des utilisateurs des noms de domaine restent en grande partie inaccessibles aux particuliers et aux entités qui servent les intérêts publics et privés légitimes.

Pour toutes les raisons mentionnées ci-dessus et au vu des missions et des objectifs approuvés par notre Conseil d'administration, nous nous voyons dans l'obligation de

[57] Consulter : https://www.icann.org/resources/board-material/resolutions-2018-05-17-en

nous opposer à l'ensemble des recommandations de politiques figurant dans le rapport final de l'étape 2.

Malgré les meilleures intentions de l'IPC et de la BC, l'expérience de l'EPDP constitue un échec. Elle s'est avérée incapable de répondre aux questions d'ordre juridique émanant du RGPD. Les régulateurs et les législateurs devraient prendre bonne note du fait que le modèle multipartite de l'ICANN s'est avéré incapable de répondre aux besoins en matière de protection des consommateurs, de cybersécurité et d'application de la loi. Par conséquent, des orientations juridiques précises de la part du RGPD s'avèrent nécessaires de même que l'exploration de voies légales et règlementaires alternatives.

Concernant la BC et l'IPC

La mission de l'unité constitutive des entreprises et des utilisateurs commerciaux (BC) telle qu'elle a été approuvée par le Conseil d'administration de l'ICANN est de *« garantir que l'ICANN s'acquitte de ses fonctions avec transparence et responsabilité et de veiller à ce que ses positions politiques soient cohérentes avec le développement de l'Internet qui (...) vise à promouvoir la confiance des utilisateurs lors de leurs interactions commerciales et communications en ligne... »*

La finalité de l'unité constitutive des représentants de la propriété intellectuelle (IPC) tel qu'approuvée par le Conseil d'administration est de *« représenter le point de vue et les intérêts des titulaires de droits de propriété intellectuelle au niveau mondial en mettant l'accent sur les marques déposées, la propriété intellectuelle et les droits de propriété intellectuelle connexes ainsi que leurs effets et leurs interactions avec le système des noms de domaine (DNS) afin de garantir que chaque point de vue, notamment ceux minoritaires, soit reflété dans les recommandations émanant du conseil de la GNSO et du Conseil d'administration de l'ICANN ».*

Déclaration minoritaire du Comité consultatif gouvernemental portant sur les données d'enregistrement des gTLD figurant dans le rapport final de l'étape 2 de l'EPDP

Note : *le Comité consultatif At-Large (ALAC), l'Unité constitutive des utilisateurs commerciaux (BC) et l'Unité constitutive des représentants de la propriété intellectuelle (IPC) appuient les points de vue exprimés dans ce commentaire.*

Introduction

Le GAC apprécie sincèrement les efforts réalisés par l'ensemble de l'équipe responsable de l'EPDP, l'engagement de ses présidents et de l'équipe de soutien de l'ICANN au cours de ces derniers 23 mois et reconnaît le temps et l'énergie considérables consacrés à l'élaboration de recommandations de politiques complexes et importantes concernant l'accès et la divulgation des données d'enregistrement de noms de domaine (auparavant connu comme WHOIS). Les statuts constitutifs de l'ICANN établissent que les données WHOIS sont nécessaires pour « les besoins légitimes en matière d'application de la loi » et pour « promouvoir la confiance du consommateur ».[58] Le GAC a également reconnu à plusieurs reprises l'importance de ces objectifs signalant que les données WHOIS sont utilisées pour un ensemble d'activités légitimes dont l'assistance aux enquêtes des forces de l'ordre, l'appui aux entreprises pour combattre la fraude et l'utilisation abusive de la propriété intellectuelle, la garantie des intérêts du public et le renforcement de la confiance des utilisateurs vis-à-vis de l'Internet en tant que source de communication et d'information fiable.[59]

Au vu de ces objectifs cruciaux, la spécification temporaire relative aux données d'enregistrement des gTLD de l'ICANN vise à « garantir, dans la mesure du possible, la continuité de la disponibilité du WHOIS tout en maintenant la sécurité et la stabilité du système d'identificateurs uniques de l'Internet ».[60] Les recommandations finales contiennent des éléments utiles qui constituent une amélioration de la spécification temporaire actuelle régissant l'accès aux données d'enregistrement des noms de domaine. Toutefois, le GAC s'abstient de soutenir certaines recommandations qui, en l'état, ne parviennent pas à l'équilibre nécessaire entre la protection des droits de ceux qui fournissent des données aux registres et aux bureaux d'enregistrement d'une part et la protection du public confronté aux dommages causés par des acteurs néfastes visant à tirer parti du système des noms de domaine, de l'autre.[61] En ce sens, le GAC

[58] Statuts constitutifs de l'ICANN, révision du service d'annuaire de données d'enregistrement, paragraphe 4.6(e).
[59] *Consulter par exemple :* Communiqué du GAC d'Abu Dhabi, chapitre VII.3 page11 et Principes du GAC concernant les services WHOIS, 2007.
[60] *Consulter la page Internet sur la protection / confidentialité des données de l'ICANN :* https://www.icann.org/dataprotectionprivacy
[61] De même que d'autres groupes de parties prenantes, le GAC s'oppose aux recommandations suivantes : 5 - Exigences de réponse ; 6 - Niveaux de priorité ; 8 - Autorisation des parties contractantes ; 14 - Viabilité financière ; 18 - Examen des recommandations de mise en œuvre des politiques portant sur le SSAD qui font appel à un

rappelle que le système des noms de domaine constitue une ressource publique mondiale devant servir les besoins de l'ensemble des utilisateurs, y compris les consommateurs, les entreprises, les titulaires de noms de domaine et les gouvernements.

Dans sa déclaration minoritaire, le GAC fait part de ses préoccupations en matière de politique publique au regard de la façon dont les recommandations finales :

1) aboutissent actuellement à un système de divulgation fragmenté et non pas centralisé,
2) ne contiennent pas de normes imposant la révision des décisions de divulgation,
3) ne répondent pas suffisamment aux inquiétudes en matière de confiance et de protection des consommateurs,
4) ne disposent pas actuellement de mécanismes fiables permettant au système normalisé d'accès et de divulgation (SSAD) d'évoluer vers de meilleures réponses du point de vue de la clarté juridique, et
5) risquent d'entraîner de telles charges financières faisant du SSAD un système dont les coûts disproportionnés pèseront sur les utilisateurs, notamment ceux en charge de détecter et de répondre aux menaces de cybersécurité.

En outre, tel que nous l'avons souligné dans notre commentaire du GAC sur le supplément au rapport initial de l'étape 2 de l'EPDP, le rapport final ne permet pas de répondre à certaines questions essentielles (notamment celles qui portent sur l'exactitude des données, le masquage des données des entités juridiques non protégées au titre du RGPD et l'utilisation d'adresses de courrier électronique anonymisées). Le modèle bénéficierait également de clarifier les statuts et les rôles de chacune des autorités de contrôle et des traiteurs. Le GAC a chargé le conseil de la GNSO de veiller à ce que ces questions cruciales soient prises en compte rapidement dans cet EDPD ainsi que dans la prochaine étape, l'étape finale 3.

Système de divulgation fragmenté

Bien que les recommandations finales fassent état d'un système centralisé pour le dépôt des requêtes, il n'existe pas de centralisation au niveau de la divulgation des données. Les recommandations, en leur état actuel, créent un système fragmenté qui entrave l'accès adéquat aux données d'enregistrement et risque de ralentir les enquêtes en matière de cybersécurité, de propriété intellectuelle et d'application de la loi. Le GAC met en garde contre la création « d'un système d'accès fragmenté basé sur des milliers de règles différentes en fonction du bureau d'enregistrement concerné » et signale que l'« absence de règles d'accès cohérentes aux informations non-publiques risque d'entraîner des retards entravant les investigations et permettant à

Comité permanent de la GNSO. Consulter la désignation par consensus de l'annexe D Rapport final de l'étape 2 de l'EPDP.

des conduites potentiellement néfastes pour le public de perdurer. [62] Selon le GAC, ce résultat ne s'inscrit pas dans l'optique d'un « mécanisme d'accès fonctionnel, prévisible et stable aux informations WHOIS non publiques ».[63] D'autre part, il est à noter que l'autorité belge de protection des données reconnaît les bénéfices potentiels d'un modèle centralisé et signale explicitement que le RGPD n'empêche point d'automatiser plusieurs fonctions du modèle de divulgation. [64]

Toutefois, les recommandations en matière de divulgation :

- dépendent presque entièrement d'évaluations et de décisions prises individuellement par plus de 2000 bureaux d'enregistrements accrédités par l'ICANN ; [65]
- ne prend pas suffisamment en compte l'automatisation des tâches puisqu'il n'existe que de deux types de réponses automatiques ; [66] et

- n'offrent pas suffisamment de mécanismes fiables permettant de multiplier les catégories de requêtes auxquelles une divulgation automatique pourrait s'appliquer suivant des orientations juridiques futures ou des modifications de l'application de la loi en matière de vie privée.[67]

Le système de divulgation fragmenté actuel et l'incertitude relative qui demeure quant à une centralisation future risquent de porter atteinte à la stabilité et à la prévisibilité du SSAD.

Absence de normes contraignantes pour l'examen des décisions de divulgation

Le GAC reconnaît qu'au titre des règles applicables en matière de protection des données, y compris le RGPD, les parties contractantes resteront responsables quant à la décision de divulguer les données d'enregistrement des noms de domaine et risquent d'encourir, de ce fait, certains risques en termes de responsabilité. Le GAC est conscient que les parties contractantes ont visé à maintenir le contrôle sur la décision de divulguer ou non les données d'enregistrement de noms de domaine. Toutefois, le GAC signale que ces décisions décentralisées de divulguer les données soustrait ce

[62] Communiqué du GAC de Barcelone (Section IV.2 Autres questions –portant sur la Spécification temporaire, page 6).
[63]Communiqué du GAC de Panama, consulter les fondements de l'avis de consensus du GAC adressé au Conseil d'administration de l'ICANN (Section V.1, page 7)
[64] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[65] Recommandation (Rec.) 8
[66] Rec. 9.41 et 9.42
[67] Rec. 8.17 et 18

mécanisme aux enjeux et aux mesures d'application de la loi, notamment en ce qui concerne le service de la conformité de l'ICANN. [68]

Les données d'enregistrement sont fondamentales pour la sécurité et la stabilité du DNS, et des inquiétudes demeurent quant au fait que les parties contractantes puissent, par inadvertance ou intentionnellement, perdre de vue l'intérêt public que représente l'accès du requérant à ces données. Le Président-directeur général de l'ICANN a récemment fait part de son inquiétude au Comité européen de la protection des données, signalant qu'« en raison de l'absence de certitude juridique, les bureaux d'enregistrement et les autorités de contrôle risquent d'interpréter la protection des données et de la vie privée en termes absolus pour éviter toute sanction règlementaire ou jugement à leur encontre et perdre de vue d'autres droits ou intérêts légitimes ».[69] Le fait d'opposer un refus à des requêtes d'accès aux données d'enregistrement des noms de domaine légitimes ont des conséquences réelles. Dans son Communiqué de Barcelone, le GAC signale que les enquêtes et les analyses montrent que la mise en œuvre de la Spécification temporaire en réponse au RGPD a eu un effet négatif sur l'application de la loi et sur la capacité des professionnels en matière de cybersécurité de mener des enquêtes et d'atténuer les actes criminels grâce à l'accès aux informations du système WHOIS autrefois disponibles au public. [70]

Les recommandations actuelles ne proposent aucun mécanisme permettant d'examiner les décisions de divulgation. En l'état actuel, le système proposé ne permet pas au service chargé de la conformité de l'ICANN d'examiner les enjeux majeurs qui sous-tendent les décisions de divulgation. En effet, le service de conformité de l'ICANN joue un rôle limité dans l'examen des plaintes visant le non-respect des exigences *en matière de procédure* ou les utilisations malveillantes systémiques.[71] Par conséquent, les recommandations du SSAD promeuvent un système qui risque d'encourager une approche conservatrice des décisions de divulgation afin de réduire les risques de

[68] Rec. 8. Rec. 5.3 et 5.4. ***Consulter également*** la lettre du Président-directeur général de l'ICANN au Comité européen de la protection des données datée du 22 mai 2020 https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf.

[69] Consulter la lettre datée du 22 mai 2020 du Président-directeur général de l'ICANN au Comité européen de la protection des données https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf (« L'absence de certitude quant à la manière d'équilibrer les intérêts légitimes d'accéder aux données d'une part, et les intérêts des individus concernés d'autre part, laisse la porte ouverte aux jugements subjectifs et à la discrétion du bureau d'enregistrement et du responsable du traitement recevant la demande pour accepter ou refuser l' accès aux données d'enregistrement gTLD non publiques »).

[70] Consulter également la section 5.2.1 du Rapport final de l'équipe de révision responsable des services d'annuaire des données d'enregistrement 2 (3 septembre 2019) et l'enquête conjointe des groupes de travail anti-abus pour la messagerie, les programmes malveillants et les mobiles (18 octobre 2018)

[71] Rec. 5.3 à 5.5. En outre, les orientations relatives à la mise en œuvre n'exigent même pas des parties prenantes qu'elles ajustent leurs analyses concernant leurs décisions de divulgation « au regard de la jurisprudence en matière d'application en interprétant les orientations relatives au RGPD émanant du CEPD, ou les révisions au RGPD ou autre loi en matière de vie privée applicable à l'avenir. *Consulter* la Rec. 8.17. Du fait de l'utilisation de l'expression « DEVRAIENT » au lieu de « DOIVENT », les orientations ne s'avèrent pas contraignantes (consulter l'e-mail adressé à l'équipe responsable de l'EPDP des représentants de l'ICANN daté du 19 décembre 2019 relatif à la force contraignante induite par l'usage des termes « DEVRAIENT » et « DOIVENT »).

devoir assumer la responsabilité et qui ne permet pas de réaliser, dans le cadre des mécanismes d'application de la loi de l'ICANN, un examen robuste des décisions de divulgation. L'octroi d'une discrétionnalité absolue aux parties contractantes pour revoir les demandes de divulgation risque de porter atteinte à l'obligation de garantir la viabilité permanente des données d'enregistrement des noms de domaine en tant qu'outil pour défendre les droits et les intérêts du public et d'assurer sa protection de même que celle des unités constitutives des représentants de la propriété intellectuelle et des utilisateurs commerciaux. Le GAC considère que cette approche risque de porter atteinte à la stabilité et à la prévisibilité du SSAD.

Rendre prioritaires les requêtes portant sur la protection des consommateurs

Le GAC a exprimé son inquiétude quant à la priorité accordée aux requêtes visant la protection des consommateurs (notamment pour ce qui est de l'hameçonnage, de l'utilisation malveillante et de la fraude) [72] laquelle soulève des questions d'intérêt public et exige des mesures immédiates. [73] Les recommandations actuelles situent les requêtes portant sur la protection des données au plus bas des trois niveaux de priorité. En outre, les exigences de niveau de service qui régissent les temps de réponse des requêtes de priorité 3 entraînent des réponses tardives : délais de cinq jours au cours des six premiers mois de mise en œuvre puis le délai de réponse double et passe à 10 jours. [74] Ce manque de hiérarchisation et les temps de réponse longs pourraient entraîner des dommages importants au vu de la rapidité avec laquelle la fraude et les cyberattaques produisent des dégâts. Le GAC recommanderait de considérer les requêtes de protection des consommateurs comme étant de priorité 2.

Même si la désignation actuelle de priorité 3 était acceptée, l'opération suggérée dans le cadre de la Recommandation 6 suscite des préoccupations. Le GAC accueille favorablement le fait que la recommandation exige au requérant la capacité de signaler les requêtes ayant soulevé des craintes liées à la protection des consommateurs (« les requérants DOIVENT avoir la capacité d'indiquer si la requête de divulgation touche à la protection des consommateurs. . . ».[75] Toutefois, la recommandation ne comporte pas d'obligation similaire exécutoire pour les parties contractantes sur le fait de donner priorité aux requêtes liées à la protection des consommateurs par rapport aux autres parties au même niveau de priorité. En lieu et place du terme « DOIVENT », les recommandations mentionnent que les parties contractantes « DEVRAIENT » donner la priorité à ce type de requêtes.[76] Or, le service

[72] Le GAC note également que la définition proposée des demandes de protection des consommateurs semble indûment restrictive et demande que la parenthèse proposée soit interprétée comme illustrative plutôt que comme exhaustive.

[73] *Consulter le* Commentaire du SSAC sur le rapport initial de l'étape 2 du processus accéléré d'élaboration de politiques concernant la Spécification temporaire relative aux données d'enregistrement des gTLD *(*SAC 111) pages 9 et 10.

[74] Rec. 6.2 et Rec. 10.4 et 10.11.

[75] Rec. 6.2.

[76] Rec. 6.2

chargé de la conformité de l'ICANN a expressément informé l'équipe responsable de l'EPDP que le terme « DEVRAIENT » ne rend pas cette mesure contraignante[77]. Ainsi, cette recommandation manque de cohérence interne en ce qu'elle exige la capacité d'identifier les problèmes de protection des consommateurs, mais elle n'oblige pas les parties contractantes à agir sur cette désignation. Les discussions de l'équipe responsable de l'EPDP sur ce sujet reflètent l'idée selon laquelle cet objectif pourrait tout simplement être atteint à l'aide d'un mécanisme de classement. Les requêtes liées à la protection des consommateurs soulèvent des questions qui affectent l'ensemble de la sécurité du DNS, d'où le GAC recommande que la hiérarchisation soir obligatoire plutôt que permissive.

Mécanismes fiables pour améliorer le SSAD

Comme tout nouveau système, la SSAD serait confrontée à des défis dans sa mise en œuvre et son application et devrait y répondre en temps opportun. Les mécanismes peuvent nécessiter des ajustements, les demandes des requérants de données peuvent fluctuer et de nouvelles utilisations inattendues pour les données peuvent apparaître, notamment en matière de cybersécurité. Par conséquent, le potentiel du SSAD de s'améliorer avec le temps, de s'ajuster à de nouveaux obstacles et de répondre à de nouvelles directives juridiques est fondamental.

En ce qui concerne l'automatisation, la recommandation finale sur les décisions de divulgation automatique impliquent de rendre automatiques toutes les catégories de requêtes qui s'avèrent « faisables du point de vue technique et commercial et permises du point de vue juridique ».[78] Bien que l'équipe responsable de l'EPDP prenne en considération tout un éventail de cas d'utilisation susceptibles d'être automatisés, dans le rapport final elle a pu s'entendre sur seulement deux à inclure dans le rapport final.[79] Certains groupes de parties prenantes, dont le GAC, avaient prévu un SSAD qui incluait davantage d'automatisation et de centralisation car, comme l'ont reconnu les représentants de l'Autorité belge de protection des données, un modèle centralisé « semble être une meilleure option de « bon sens » en termes de sécurité et pour les personnes concernées ». [80] Quoiqu'il en soit, le GAC et d'autres groupes de parties prenantes sont parvenus à un accord sur ce modèle plus « hybride » que centralisé, tant que les recommandations finales incluaient un mécanisme suffisamment flexible pour que le SSAD puisse évoluer sans avoir à recourir à un PDP cohérent avec le rapport final.

La Recommandation 18 crée un Comité permanent composé de représentants de toutes les parties prenantes qui participent à l'EPDP pour s'attaquer à ces décisions.

---

77 *Consulter ci-dessus la note de bas de page 14*

78 Rec. 9.3.

79 *Consulter* les Rec. 9.41 et 9.42 (9.43 et 9.44 concernent les seules catégories de requêtes liées au champ « ville » ou aux enregistrements ne contenant pas de données à caractère personnel).

80 https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

Toutefois, le GAC considère que la Recommandation 18, portant sur la révision des recommandations de mise en œuvre des politiques, semble manquer son objectif de prévoir un mécanisme efficient qui permette l'évolution du SSAD. En particulier, il n'est pas clair si l'automatisation des nouveaux cas d'utilisation implique de nouvelles politiques ou la mise en œuvre de politiques existantes. Le GAC fait remarquer que si chaque nouveau cas d'utilisation entraîne une nouvelle politique requérant un nouveau PDP, cela remet en doute la capacité du SSAD à évoluer efficacement et notamment vers un système plus centralisé. Dans ce cas de figure, le SSAD risque de rester un système fragmenté avec toutes les inquiétudes que cette fragmentation suscite. Par conséquent, le GAC demande à la GNSO de veiller à ce que les recommandations de l'EPDP soient suffisamment claires à ce niveau et permettent de rendre automatiques les éléments futurs, une fois le test de « faisabilité commerciale et technique et d'autorisation légale » approuvé.

Toute autre proposition de changement requiert l'obtention d'un consensus au sein du Comité permanent ainsi que l'approbation des parties contractantes. Avant d'être adoptées, les recommandations devront donc être approuvées par le conseil de la GNSO (lequel ne prévoit pas de représentation des comités consultatifs). Ce processus « évolutif » pourrait devenir complexe et long et n'est pas adapté aux aspects de mise en œuvre requérant des actions décisives et rapides.

Viabilité financière

Les recommandations risquent d'aboutir à un système trop coûteux pour les utilisateurs pour lesquels il est destiné, y compris les utilisateurs du SSAD qui enquêtent et combattent les menaces en matière de cybersécurité. Les recommandations préconisent que « les personnes concernées NE DOIVENT PAS payer le coût de la divulgation des données aux tierces parties ; les personnes requérant des données du SSAD devraient être les premières à assumer les coûts associés à l'entretien du système »[81]. Bien que le GAC reconnaisse la demande de ne pas faire payer les titulaires de noms de domaine lorsque d'autres souhaitent accéder à leurs données, il note également que les titulaires de noms de domaine assument les coûts des services d'enregistrement de domaines dans leur ensemble lorsqu'ils enregistrent un nom de domaine. Tel que le SSAC l'a fait récemment remarquer :

> Ces coûts devraient inclure les divulgations à des tiers ayant le droit d'obtenir les données expurgées afin de mener à bien des activités légitimes en matière de sécurité, stabilité et résilience (SSR) et d'autres activités juridiques potentielles (par exemple, la protection des droits) qui ne sont pas dans le champ d'action du SSAC. En termes généraux, la sécurité, la stabilité et la résilience du DNS requièrent l'accès à ce type de données afin de permettre

[81] Rec. 14.2.

> les communications entre les propriétaires des ressources compromises et l'identification des activités malicieuses et frauduleuses en vue de suspendre des services d'enregistrement obtenus par les auteurs de délits. [82]

En outre, le GAC remarque qu'une grande partie des dépenses du SSAD est liée à son utilisation généralisée du traitement manuel (par opposition au traitement automatisé), une approche avec une évolutivité limitée par nature et un coût intrinsèquement élevé. La durabilité financière du SSAD ne peut pas être séparée de sa dépendance du traitement manuel. Le fait de limiter, dans la mesure du possible, le fonctionnement manuel contribuera à la viabilité financière du SSAD [83]. Dans leur ensemble, les recommandations touchant au financement du SSAD peuvent être difficiles à mettre en œuvre et soulèvent plus de doutes qu'elles n'apportent de réponses, notamment quand il s'agit de savoir 1) dans quelle mesure l'ICANN peut-elle subventionner le système ? 2) dans quelle mesure les titulaires de noms de domaines peuvent-ils transférer le coût du SSAD à leurs clients ? 3) quel sera le rôle joué par les requérants dans la définition et l'approbation des frais du système, etc. ? Le GAC considère qu'une « évaluation formelle de l'impact sur l'utilisateur et en termes de sécurité et de stabilité » est souhaitable. [84]

Aspects non traités dans le rapport final de l'étape 2 de l'EPDP

Exactitude des données

En vertu de sa charte, l'équipe responsable de l'EPDP a été chargée d'évaluer le ou les « cadres pour la divulgation […] afin de traiter des (i) questions liées à l'abus des enregistrements de noms de domaine, dont la liste non exhaustive comprend la protection du consommateur, l'enquête en matière de cybercriminalité, l'utilisation malveillante du DNS et la protection de la propriété intellectuelle [et] (ii) des besoins en matière d'application de la loi. . . » L'efficacité des données d'enregistrement de noms de domaine à ces fins (en fait, à quelque fin que ce soit, y compris la capacité des parties contractantes à joindre leurs clients) dépend de l'exactitude des données. De plus, l'exactitude des données d'enregistrement est un critère essentiel du RGPD et le rapport final de l'étape 1 de l'EPDP fait état que « *le thème de l'exactitude et son rapport avec la conformité au RGPD doit être analysé davantage. . .* » En ce sens, le GAC s'inquiète de l'absence de recommandations portant sur ce sujet essentiel dans le rapport final.

Tel que le GAC l'a signalé précédemment :

---

[82] SAC 111.

[83] Afin d'encourager un traitement moins manuel il faudrait explorer les mécanismes juridiques permettant aux parties contractantes de mettre en œuvre une autorisation pour que les personnes concernées puissent donner leur consentement ou s'opposer gratuitement à la divulgation de leurs données lors de l'enregistrement de leur nom de domaine. Cela permettrait de faciliter l'entretien des bases de données, qu'elles soient ou non protégées, rendant les données non protégées disponibles à un traitement automatique, moins coûteux.

[84] *Consulter* le SAC 111.

> L'exactitude des données d'enregistrement des noms de domaine est essentielle aussi bien pour le RGPD que pour l'objectif de garantir la sécurité et la résilience du DNS. Le RGPD, ainsi que d'autres régimes de protection des données et le contrat d'accréditation de bureau d'enregistrement, exige l'exactitude des données qui est critique pour le mandat de l'ICANN qui consiste à assurer la sécurité, la stabilité et la résilience du DNS. Tel que l'énonce la Commission Européenne dans sa lettre à l'ICANN du 7 février 2018 : « Tel *que stipulé dans le cadre juridique de protection des données de l'UE et en ligne avec les obligations des parties contractantes au titre de leurs contrats avec l'ICANN, les données à caractère personnel doivent être exactes et actualisées. Toutes les mesures raisonnables doivent être prises afin de garantir que les données à caractère personnel qui s'avèrent inexactes, au regard de l'objectif pour lequel celles-ci sont traitées, soient effacées ou rectifiées dans les plus brefs délais […]. Conformément au principe de qualité des données, toutes les mesures raisonnables doivent être prises afin de garantir l'exactitude de toute donnée à caractère personnel obtenue* ».[85]

Conformément au RGPD, il est essentiel que l'exactitude et la qualité des données soient assurées « par rapport à la finalité pour laquelle elles [les données] sont traitées ».[86] La divulgation de données inexactes irait à l'encontre de l'objectif du SSAD et risquerait de violer les règles de protection des données. L'exactitude est un principe essentiel de la protection des données, inscrit dans la plupart des lois en matière de protection des données du monde entier. L'exigence d'exactitude figure notamment au Chapitre 5 du RGPD.

L'efficacité des exigences actuelles du contrat en place pour promouvoir l'exactitude de WHOIS semble incertaine. Les récents rapports des équipes de révision soulèvent des interrogations quant à l'efficacité des procédures de vérification tel que les rapports des équipes de révision du RDS et de la CCT, tous deux approuvés par le GAC. [87] En

---

85 Commentaire du GAC sur le supplément de l'étape 2.

86 *Consulter* l'article 5(1)(d) du RGPD. *Consulter également* le Guide du Bureau de la commission d'information du Royaume-Uni portant sur les orientations en matière de RGPD pour les organisations, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

87 *Consulter* par exemple le Rapport final de la révision des services d'annuaire de données d'enregistrement / WHOIS 2 pages 49 à 61 (remarque : l'inexactitude des données WHOIS est toujours élevée et probablement insuffisamment signalée) ; les Commentaires du Comité consultatif gouvernemental sur le rapport final de l'équipe de révision du RDS/WHOIS2 , datés du 23 décembre 2019, pages 5 à 7 ; le Rapport final de l'équipe de révision de la concurrence, la confiance et le choix du consommateur pages 103 à 106. *Consulter également* le Rapport de l'équipe de révision du WHOIS (11 mai 2012) pages 11 à 13 (« le faible degré d'exactitude des données WHOIS est inacceptable et porte atteinte à la confiance des consommateurs vis-à-vis du WHOIS, dans un secteur où l'ICANN définit et coordonne les règles, c'est-à-dire, au niveau de l'organisation ICANN elle-même »).

outre, depuis 2014, l'exactitude du WHOIS constitue la principale source des plaintes parmi celles informées par le service de la conformité de l'ICANN concernant les bureaux d'enregistrement. [88]

Le GAC demande donc au conseil de la GNSO de veiller à ce que, dans le cadre de l'EPDP actuel, l'exactitude des données soit une composante à part entière du SSAD.

Distinction entre personne morale et personne physique

Dans son Communiqué du GAC de l'ICANN68 daté du 27 juin 2020, le GAC a demandé à la GNSO de fournir une actualisation, dans les plus brefs délais, des progrès accomplis en vue de développer un plan spécifique pour faire avancer le processus d'élaboration de politiques pour préciser enfin le cas de figure distinct s'agissant d'une personne physique ou morale. Ce point est important car les règlements en matière de protection des données à caractère personnel, y compris le RGPD, ne s'appliquent et ne protègent que celles des personnes physiques.[89] Les informations portant sur les personnes morales ne sont pas considérées comme des données à caractère personnel couvertes par les règlementations en la matière, y compris le RGPD, tant qu'elles n'entraînent pas l'identification d'individus. Ainsi, les parties contractantes peuvent rendre publiques ces données sans que cela suscite des difficultés au niveau de la protection des données. Toutefois, tel que cela figure dans le rapport final, les bureaux d'enregistrement et les opérateurs de registre ne sont toujours pas *obligés,* mais seulement *autorisés,* à établir une distinction entre les enregistrements de personnes physiques et de personnes morales.[90] Cette pratique ne permet pas de « garantir une disponibilité permanente du WHOIS au plus haut degré possible » [91] et l'absence de procédures recommandées qui puissent s'appliquer pour faire cette distinction dans le rapport final constitue un manquement à la directive expresse de l'équipe responsable de l'EPDP et de la charte encadrant sa mission.[92]

Le masquage de données pouvant être, en toute légalité, disponible au public a un grand impact au vu du grand nombre de domaines qui sont enregistrés par les

[88] Consulter les rapports annuels du service de la conformité contractuelle de l'ICANN, détails du rapport portant sur les bureaux d'enregistrement, 2014 à 2019, https://features.icann.org/compliance/dashboard/report-list.

[89] [89] Le RGPD ne couvre pas le traitement de données à caractère personnel ayant trait aux personnes morales et notamment les démarches d'établissement d'une entité morale y compris le nom et le type d'entité morale et les détails de contact de la personne morale (considérant 14 du RGPD). « Bien que les détails de contact d'une personne morale échappent à la portée du RGPD, les détails de contact portant sur les personnes physiques en font partie, de même que toute autre information liée à une personne identifiée ou identifiable » (*Consulter* la lettre du CEPD à l'ICANN du 5 juillet 2018).

[90] Consulter la section 2.3 du rapport final de l'étape 2 de l'EPDP, thèmes de priorité 1 et 2.

[91] *Consulter sur le site internet de l'ICANN les aspects liés à la protection des données/vie privée* https://www.icann.org/dataprotectionprivacy

[92] *Consulter la charte de l'équipe responsable de l'EPDP.* https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf (y compris les instructions pour que l'équipe évalue si les parties contractantes devraient être autorisées à traiter différemment les personnes physiques et morales, ou si elles sont tenues de le faire, et le mécanisme permettant de garantir une détermination du statut fiable).

personnes morales. Une étude commandée par l'ICANN en 2013 a montré que **les personnes morales constituent le plus grand pourcentage de titulaires de noms de domaine.**[93] Une des façons pour que le public, évalue la légitimité d'un site Web et pour que les autorités d'application de la loi sachent à quelle entité il appartient est de consulter les informations disponibles portant sur le registre du nom de domaine, qui devraient inclure les données concernant les personnes morales.

Il est à noter que l'équipe responsable de l'EPDP a reçu des orientations juridiques qui suggèrent différentes mesures pour réduire les risques en matière de responsabilité. [94] Ces orientations laissent entendre qu'une grande variété de mesures permettent aux titulaires des noms de domaine de se désigner, à juste titre, en tant que personnes morales. Remarquons que certains ccTLD (y compris ceux basés dans l'UE) rendent déjà publiques certaines données concernant des personnes morales titulaires de noms de domaine, et démontrent ainsi que cette distinction est autant faisable que légale. [95]

La distinction entre les personnes morales et les personnes physiques est également lié à la question du traitement automatique des données. Tel que signalé, les personnes morales ne sont pas protégées au titre du RGPD. Ainsi, la distinction entre personnes morales et personnes physiques lors du processus d'enregistrement pourrait impliquer d'assigner aux personnes morales une catégorie en vertu de laquelle leurs données peuvent être traitées de façon automatique.[96]

Le GAC considère qu'il est essentiel de résoudre la question du statut des personnes morales et des personnes physiques pour que l'ensemble du SSAD puisse atteindre ses

---

93 *Consulter l'étude sur l'identification des titulaires de noms de domaine du WHOIS :* https://gnso.icann.org/sites/default/files/filefield_39861/registrant-identification-summary- 23may13-en.pdf (D'après notre analyse des enregistrements WHOIS extraits d'un échantillon aléatoire de 1600 domaines appartenant aux 5 principaux gTLD,

- 39 pour cent (± 2,4 pour cent) figurent enregistrés par une personne morale
- 33 pour cent (± 2,3 pour cent) figurent enregistrés par une personne physique
- 20 pour cent (± 2,0 pour cent) figurent enregistrés à travers un service d'anonymisation ou d'enregistrement fiduciaire.
- Les 8 pour cent (± 1,4 pour cent) restants n'ont pu être classés à l'aide des données WHOIS disponibles.

94 *Consulter* l'Avis en matière de responsabilité en lien avec l'auto-identification des titulaires de noms de domaine comme personnes physiques ou morales, conformément au Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD ») émis par Bird & Bird (la méthodologie recommandée propose de développer un langage de notification clair afin d'éviter les erreurs de la part des titulaires de noms de domaine et de s'assurer qu'ils comprennent parfaitement les conséquences d'un enregistrement en tant que personne morale ; vérifier que les informations de contact ne contiennent pas de données à caractère personnel).

95 *Consulter notamment* : Belgique (.BE), Union Européenne (.EU), Estonie (.EE), Finlande (.FI), France (.FR), Norvège (.NO), etc.

96 Comme garantie, les personnes disposant de protections légales renforcées pourraient se voir assignées à un groupe dont les requêtes sont traitées de façon non-automatique. Il peut s'agir de personnes morales protégées par une loi nationale (telle que le secret bancaire), ou de personnes physiques bénéficiant de protection juridique telles que des ordonnances préventives, une personne concernée au statut vulnérable (par exemple des enfants, des demandeurs d'asile ou d'autres catégories protégées) ainsi que des populations nationales de juridictions affirmant, par défaut, le droit à la vie privée.

objectifs conformément aux lois applicables en matière de protection des données en vigueur. Le GAC demande donc au conseil de la GNSO de faire tout ce qui est à sa portée pour résoudre cette question. En ce sens, le GAC réitère sa demande auprès de l'équipe responsable de l'EPDP pour qu'elle se penche sur les orientations juridiques fournies afin de développer des politiques raisonnables permettant aux informations des personnes morales de demeurer publiques.

Anonymisation des adresses électroniques

Le recours à des adresses électroniques anonymisées peut constituer un moyen de protéger l'identité des titulaires de noms de domaine tout en remplissant certains des objectifs légitimes des e requérants souhaitant accéder aux données d'enregistrement de noms de domaines. Le rapport final répertorie parmi les sujets de priorité 2 la « faisabilité de disposer d'une adresse électronique anonymisée uniforme pour les contacts uniques ».[97] L'équipe responsable de l'EPDP a reçu des orientations juridiques stipulant que l'anonymisation et pseudonymisation constituent « une mesure efficace pour le respect de la vie privée dès la conception ».[98] Tout comme ces orientations juridiques, le GAC signale que l'anonymisation de l'information échappe à la portée du RGPD. [99] Bien que le GAC reconnaisse la possibilité d'établir un lien entre l'information anonyme et les données à caractère personnel, il approuve l'orientation juridique selon laquelle l'anonymisation serait une technique utile pour renforcer la protection de la vie privée, et en tant que telle, devant être examinée plus profondément.

À la lumière de ce qui figure ci-dessus, le GAC considère qu'une analyse de faisabilité supplémentaire est nécessaire pour mieux comprendre les risques et les bénéfices de cette option et ne pas l'éliminer d'emblée.

97 Rapport final de l'étape 2 de l'EPDP, page 3.

98 Bird & Bird Avis juridique, « Lot 2 » de questions à propos du RGPD portant sur un système normalisé d'accès et de divulgation (« SSAD »), adresses électroniques pseudonymisées et enregistrement fiduciaire ou anonymisé » (4 février 2020).

99 *Consulter* le considérant 26 au RGPD.

Responsabilité de contrôle du traitement

La possible responsabilité conjointe du traitement entre les parties contractantes et l'ICANN figure dans le rapport final. Le GAC souhaiterait néanmoins davantage de clarté concernant le statut et le rôle de chacune des autorités de contrôle et de traitement du modèle du SSAD. En particulier, le fait de mettre en place des accords concrets pour le traitement des données permettrait de démontrer plus clairement la façon dont la responsabilité se partage, au niveau des différentes opérations de traitement des données, entre les parties contractantes et l'organisation ICANN. Le GAC encourage également le conseil de la GNSO à demander à l'EPDP d'examiner davantage cette question.

Conclusion

Le GAC se félicite des efforts de bonne foi consentis par les parties prenantes, le personnel et les présidents de l'EPDP ayant pris part à l'étape 2 de l'EPDP et de leur dévouement soutenu pour faire avancer cette question de politique publique fondamentale. Le rapport final contient beaucoup d'éléments louables. Toutefois, le GAC considère que certaines recommandations clé et certains points restés sans réponses requièrent des travaux supplémentaires et que, en ce sens, le conseil de la GNSO doit demander à l'équipe responsable de l'EPDP d'achever ses travaux en tenant compte des points soulevés dans les déclarations minoritaires. Le GAC se réjouit de l'engagement permanent de tous les collègues au sujet de ces thèmes cruciaux.

Déclaration minoritaire du groupe des représentants des entités non commerciales (NCSG)

Le NCSG n'a pas approuvé les Recommandations 22, 20 et 7 pour les raisons détaillées ci-dessous.

Recommandation 22 : Finalité 2

La finalité 2 telle qu'elle figure actuellement dans la Recommandation 22 préconise de : *« contribuer au maintien de la sécurité, la stabilité et la résilience du système des noms de domaine, conformément à la mission de l'ICANN ».*

Le NCSG s'oppose fermement à cette finalité. Celle-ci s'avère bien trop vague et ouverte, permettant à l'ICANN de traiter les données d'enregistrement des gTLD comme bon lui semble. Il suffit pour cela à l'organisation ICANN d'invoquer une raison cohérente avec l'interprétation faite de ses statuts constitutifs, tel qu'a pu l'admettre Becky Burr dans un courrier électronique envoyé à l'équipe responsable de l'EPDP au nom du Conseil d'administration de l'ICANN.

Dans ledit courriel, Mme. Burr déclare que « *la SSR fait partie de la mission de l'ICANN, comme l'indiquent ses statuts constitutifs. Au chapitre 1, article 1.1 des statuts constitutifs de l'ICANN, il est clairement stipulé que l'ICANN a pour mission de garantir des opérations stables et sûres (SSR) du système unique d'identificateurs d'Internet. Les statuts constitutifs contiennent eux-mêmes des détails significatifs concernant la portée de la mission s'agissant des noms, du système des serveurs racine, des numéros et des protocoles ».*

Dans l'étape 1 nous avons développé une fiche de travail pour chacune des finalités de l'ICANN détaillant les fondements juridiques et les activités liées au traitement de chacune d'entre elles. L'étape 2 a omis de le faire. Par conséquent, la reformulation de la finalité 2 n'explicite pas les raisons de la divulgation des données, ni la manière dont elles seront retenues, ni pour combien de temps. La finalité 2, telle qu'elle est esquissée dans le rapport final de l'étape 2, entre à son tour en conflit avec le principe de la limitation de la finalité de l'article 5(1)(b) du RGPD, qui exige que les données soient *« collectées pour des finalités légitimes, explicites et spécifiées et ne subissent pas de traitement ultérieur pour un but incompatible avec celui affiché »*. La garantie des opérations stables et sûres (SSR) du système d'identificateurs uniques d'Internet n'est guère spécifique ni explicite, encore moins en raison de l'interprétation du Conseil d'administration de l'ICANN selon laquelle la SSR relèverait de sa compétence.

Le NCSG a demandé à plusieurs reprises à l'équipe responsable de l'EPDP de définir clairement la mission de l'ICANN concernant la SSR et la façon dont elle l'applique au traitement des données d'enregistrement des gTLD. Bien que devant être acquittées

par l'ICANN pour remplir ses obligations légales en tant qu'autorité de contrôle des données à ce niveau, ces requêtes furent systématiquement rejetées.

L'équipe responsable de l'EPDP n'est pas parvenue à un accord sur la façon dont les SSR s'appliquent à ce but dans le cadre de la mission de l'ICANN, et cette dernière ne semble pas avoir le moindre élément de réponse. Toutefois, comme dans le cas d'autres fondements juridiques, l'article 6(1)(f) du RGPD crée des obligations supplémentaires de la part des autorités de contrôle vis-à-vis des personnes concernées, y compris la protection de leurs droits et de leurs intérêts.

Dans ses directives sur l'utilisation de l'article 6(1)(f) en tant que fondement juridique , le bureau du commissaire aux informations du Royaume-Uni considère que ce fondement juridique est le plus approprié lorsque (parmi d'autres circonstances) l'utilisation des données se fait à un moment où les individus s'y attendent et que leurs répercussions au niveau de la vie privée est minime. D'après la finalité 2, il est pratiquement impossible aux titulaires de gTLD de savoir la façon et les raisons qui poussent l'ICANN à divulguer ou à retenir leurs données. Ces circonstances inconnues n'ont été identifiées ni par l'ICANN ni par l'équipe responsable de l'EPDP et la seule façon pour un titulaire de nom de domaine de s'y retrouver serait que, lors de l'enregistrement d'un gTLD, le titulaire puisse devenir expert dans l'interprétation et l'application des statuts constitutifs de l'ICANN. Cette attente n'est pas réaliste et excède les capacités du personnel, des membres du Conseil d'administration de l'ICANN et des membres de l'équipe responsable de l'EPDP.

Le NCSG considère que cette finalité n'est pas nécessaire pour que l'ICANN remplisse sa mission. Sa raison d'être est de satisfaire les désirs des tiers, bien que la référence aux intérêts légitimes de ces parties ait été éliminée des recommandations revues. Le Conseil d'administration de l'ICANN se croit couvert par ce fondement juridique en termes de responsabilité, ce qui n'est probablement pas le cas, tout en négligeant les intérêts des personnes concernées que le RGPD est pourtant sensé autonomiser.

Pour que cette finalité soit juste vis-à-vis des titulaires de noms de domaine, elle doit être ventilée en de multiples finalités bien définies qui permettent d'identifier clairement les activités liées au traitement qui seront communiquées et expliquées aux titulaires afin qu'ils puissent les comprendre aisément.

Recommandation 20 : Champ « ville »

Le NCSG considère qu'il n'existe pas de bonnes raisons pour remplacer, dans les recommandations faites au niveau du champ « ville » dans l'étape 1 de l'EPDP, le terme « DOIT » par « POURRAIT ». La recommandation antérieure qui demandait l'expurgation de ce champ reposait sur l'avis juridique de Bird & Bird rédigé ainsi :

« 3.16 Prenant en considération tout ce qui a été dit ci-dessus, les parties contractantes doivent réussir le test des intérêts légitimes justifiant la publication du champ « ville ». Toutefois, d'après les informations qui nous ont été fournies jusqu'à présent, cela n'apparait pas clairement. En particulier :

a) des informations complémentaires sont requises pour démontrer que les bénéfices pour les détenteurs de droits ne sont pas seulement utiles pour quelques cas limités et justifient une publication universelle du champ « ville » ; et

b) des informations sur les répercussions potentielles au niveau des droits et des intérêts des sujets concernés sont requises.

3.17 Les parties pertinentes devront ensuite mener une évaluation détaillée des faits et des circonstances afin de définir si les intérêts poursuivis surpassent ceux des sujets concernés ».

Ces éléments démontrent la nécessité de faire un test d'équilibre afin de comparer les intérêts légitimes des tiers requérant la divulgation des données d'enregistrement des gTLD et les droits des titulaires concernés. Le NCSG croit fermement que ce test doit être réalisé dans le cadre du traitement des requêtes de divulgation via le SSAD et ne doit pas être confondu avec les objectifs poursuivis par l'ICANN dans le traitement des données d'enregistrement des gTLD tel que cela figure dans les recommandations de l'étape 1 de l'EPDP.

Ces conclusions auxquelles aboutit Bird & Bird sont réaffirmées dans leur e-mail à Kurt Pritz, dans lequel ils déclarent que « *les analyses juridiques sont claires - il s'agit de données à caractère personnel. Leur publication peut être en principe justifiée sur la base des intérêts des titulaires de droits, à moins que les intérêts des individus ne les supplantent.*

La façon dont cela s'applique aux faits - déterminer si l'intérêt des titulaires de droits est suffisant et le concilier avec les intérêts des titulaires de noms de domaine - n'est pas clairement définie ».

Ceci indique clairement que le champ « ville » des données d'enregistrement des gTLD doit être traité comme le reste des informations à caractère personnel, et DOIT donc être expurgé.

Recommandation 7 : finalités du requérant

Le NCSG réaffirme son désaccord concernant le fait d'inclure la directive UE NIS dans une note en bas de page à titre d'exemple législatif portant obligation pour les organes de règlementation auxquels elle s'applique. Cet exemple a été ajouté à la

recommandation lors d’une étape de travail de l’équipe responsable de l’EPDP visant à peaufiner les recommandations et le rapport final afin d’obtenir le maximum de soutien ; le NCSG considère qu’il n’a pas bénéficié du temps et de l’attention nécessaires avant d’être inclus dans le rapport final, tout comme les implications d’une politique permettant la divulgation aux tiers.

En outre, le NCSG considère que le fait d’exclure cet exemple n’aura pas de répercussion concrète au niveau de la capacité des organes de règlementation concernés par la directive NIS ou tout autre législation de ce genre d’exiger la divulgation des données d’enregistrement des gTLD expurgées du SSAD.

Déclaration minoritaire du groupe des représentants des bureaux d'enregistrement (RrSG)

Le rapport final de l'étape 2 de l'EPDP représente l'aboutissement d'années de collaboration au sein de la communauté de l'ICANN. Le RrSG continue de croire qu'il est dans l'intérêt de tous de créer des politiques et un système permettant d'équilibrer les exigences en matière de protection des données des titulaires de noms de domaine avec les besoins de ceux qui comptent sur l'accès aux données d'enregistrement non publiques pour des finalités légales et légitimes.

Les bureaux d'enregistrement ont exprimé des préoccupations sincères tout au long du processus de l'étape 2 de l'EPDP concernant la légalité, la faisabilité technique et les coûts associés au développement, au déploiement et à l'exploitation du SSAD. Tandis que les bureaux d'enregistrement appuient certaines recommandations plus que d'autres, les recommandations étant interdépendantes, elles doivent être considérées dans leur ensemble, leur somme finale étant supérieure à la somme de ses parties.

Ainsi, dans l'optique d'un compromis continu auprès des parties prenantes et de leurs intérêts, nous appuyons le résultat de l'étape 2 de l'EPDP et les recommandations de son rapport final et nous nous engageons à suivre les politiques de consensus qui en résulteront.

Nous considérons que les recommandations finales fournissent suffisamment d'orientations sur lesquelles faire reposer un système prévisible et normalisé et donnent suite aux recommandations de l'étape 1 de l'EPDP tout en laissant la flexibilité suffisante pour que chacun des bureaux d'enregistrement mette en œuvre ses opérations dans le cadre du SSAD de manière à ce que celles-ci soient conformes à leurs autres obligations juridiques, portant souvent sur plusieurs juridictions, en matière de vie privée.

Nous exhortons le conseil de la GNSO et le Conseil d'administration de l'ICANN à adopter l'ensemble des recommandations figurant dans le rapport afin d'engager la mise en œuvre des travaux et les expéditions de lancement du SSAD.

Déclaration du Groupe des représentants des opérateurs de registres à propos du rapport final de l'étape 2 de l'EPDP

Le groupe des représentants des opérateurs de registres (« RySG ») apprécient les travaux réalisés dans le cadre de l'étape 2, reconnaissent l'utilité du SSAD pour les parties tierces et soutiennent les recommandations contenues dans le rapport final. Les recommandations reflètent les efforts déployés par l'équipe responsable de l'EPDP pour développer un accès aux données personnelles permettant d'équilibrer les droits à la vie privée des sujets concernés avec les intérêts légitimes des tiers. Bien que cette déclaration mentionne des préoccupations quant à certains aspects du rapport final, nous acceptons pour autant le compromis que constituent les recommandations définissant les bases du SSAD. Nous restons optimistes quant au développement futur du SSAD.

Pendant près d'une année de diligence, les bureaux d'enregistrement ont soutenu fermement que ce système devait (i) refléter la réalité des lois actuelles en matière de protection des données, (ii) hiérarchiser et protéger correctement les données à caractère personnel des titulaires de noms de domaine avant les intérêts des tierces parties, et (iii) garder notre capacité en tant qu'autorité de contrôle de nous acquitter de nos obligations légales en matière de protection des données à caractère personnel. Certains ont exprimé leurs réticences vis-à-vis d'un système reposant sur ces principes. Nous nous sentons satisfaits de partir de ces principes que nous considérons incarner la meilleure façon de protéger les données à caractère personnel des titulaires de noms de domaine tout en remplissant nos obligations juridiques.

Participation en toute bonne foi du RySG

L'équipe responsable de l'EPDP a pour mission de « déterminer si la Spécification temporaire relative aux données d'enregistrement des gTLD doit devenir une politique de consensus de l'ICANN, en l'état ou avec des modifications, tout en étant conforme au RGPD et à d'autres lois et règlementations applicables en matière de protection des données et de la vie privée »[100]. La charte stipule que les travaux secondaires d'évaluation d'un système pour le bénéfice des tiers et leur accès aux données à caractère personnel des titulaires de noms de domaine ne débutera que lorsque les questions primordiales « seront répondues en vue du rapport initial sur la Spécification temporaire.[101] Le rapport final de l'étape 1, paru le 19 février 2019, comprend une recommandation détaillée et applicable pour la normalisation des processus permettant aux tiers d'obtenir les données à caractère personnel des titulaires de noms de domaine.[102]

[100]Charte finale de l'EPDP adoptée le 19 juillet 2018, disponible ici.
[101]Charte finale de l'EPDP adoptée le 19 juillet 2018, disponible ici.
[102] *Consulter* le rapport final de l'étape 1 de l'EPDP, Recommandation 18, disponible ici.

Un tel système n'est pas nécessaire au niveau de nos registres pour que nous puissions nous acquitter de notre obligation de protéger les données à caractère personnel des titulaires de noms de domaine et répondre aux requêtes des tiers visant à obtenir ces données. Alors que nous ne disposons pas actuellement de SSAD, nos membres répondent de façon régulière et en faisant preuve de responsabilité aux demandes de données en vertu des exigences du rapport de l'étape 1 et de nos obligations face à la loi. Et nous continuerons de le faire même lorsque le SSAD sera opérationnel. Malheureusement, par bien des aspects, le SSAD rendra notre tâche moins aisée en ajoutant des instances de traitement supplémentaires et des risques pour les données à caractère personnel des titulaires de noms de domaine.

Nous avons accueilli avec l'esprit grand ouvert les propos des communautés visant à avoir davantage d'accès aux données à caractère personnel et nous avons participé à ce processus en vue de trouver des solutions. Bien que nous appuyions le rapport final et les nombreux compromis faits par le groupe, à l'heure où la communauté se tourne vers la mise en œuvre nous restons préoccupés pour des raisons que nous énumérons ci-dessous et qui demandent toute notre attention.

Priorités du RySG en termes de protection des données

D'emblée, nous avons mis les principes de la protection des données au cœur de ces discussions. La protection des données en général et le RGPD en particulier « protègent les droits fondamentaux et les libertés des personnes physiques, notamment leur droit à la protection des données à caractère personnel » [103]. Tel que la Commission de l'UE l'a récemment répété, « l'objectif ultime du RGPD est de changer la culture et le comportement de tous les acteurs impliqués *dans l'intérêt des personnes »*[104]*.* Pour le dire simplement, l'objectif de la protection des données est de protéger les données à caractère personnel des individus. Aussi incontestable que ce principe puisse nous sembler, notre expérience des deux dernières années nous montre pourtant un autre tableau.[105]

Dans la pratique, accorder la priorité à la protection des données implique de placer au premier plan les personnes concernées, les conséquences de la façon dont leurs données sont traitées et de qui s'en charge. Cela implique de privilégier par défaut la minimisation de données et la protection de la vie privée en évitant tout traitement non nécessaire des données à caractère personnel. Cela implique également d'éviter les conditions politiques entravant nos capacités à nous acquitter de l'obligation de

[103] Article 1(2) du RGPD

[104] Communication de la Commission au Parlement et au Conseil européens, Commission européenne, datée du 24 juin 2020, page 5 (accent d'intensité ajouté), disponible ici.

[105] Bien que le chapitre 17 de la Charte des droits fondamentaux reconnaisse que « la propriété intellectuelle doit être protégée », le Parlement européen a précisé que l'exercice de ce droit « ne doit pas entraver [. . .] la protection des données à caractère personnel, y compris sur Internet. Consulter la Directive 2004/48/EC du Parlement et du Conseil européens du 29 avril 2004 sur l'application des droits de propriété intellectuelle, disponible ici.

veiller aux données à caractère personnel qui nous incombe en tant qu'autorité de contrôle.

Tout en gardant ces principes à l'esprit, nous avons fait preuve, à de nombreuses reprises, de flexibilité et œuvré afin de prendre en considération les intérêts des tiers bien que cela nous oblige à faire des concessions pouvant accroitre les risques pesant sur les parties contractantes. Bien que certaines parties auraient souhaité aller plus loin, nous avons dû imposer nos limites face à la demande de réaliser des compromis sur certains domaines - le conseil juridique indépendant de l'étape 2, les autorités de protection des données, et nos propres membres de la CPH experts en législation concernant la protection des données de l'UE l'ont suffisamment répété- échappant à la licéité ou représentant un risque élevé pour les personnes concernées.

Le but de l'étape 2 était de normaliser le processus de requête des données à caractère personnel des titulaires de noms de domaine pour les tiers. Cependant, après des mois et des mois de persévérance et d'analyses, l'automatisation potentielle de l'accès virtuel aux données à caractère personnel ne s'avère pas bénéfique pour les personnes concernées. Les tentatives pour obtenir à tout prix un accès automatique risquent de porter atteinte à la viabilité future et à la licéité du SSAD.

Le modèle hybride reflète la réalité pratique et juridique

Le modèle hybride (avec une saisie centralisée et une prise de décision décentralisée) constitue une solution pratique qui nous semble à même de résoudre plusieurs difficultés que les requérants ont invoquées vis-à-vis du statut quo régissant la méthode d'accès aux données à caractère personnel des titulaires de noms de domaine. Plus important encore, le modèle hybride reflète la réalité de ce qui est actuellement possible face à la loi.

Le cabinet Bird & Bird a confirmé la responsabilité qui incombe aux autorités de contrôle des données et, dans l'éventualité d'un système entièrement automatisé et centralisé limitant la marge de manœuvre des parties contractantes, « le résultat le plus probable - du fait notamment de la position de départ de la majorité des autorités de supervision - sera que les CP deviennent des autorités de contrôle »[106]. En outre, l'autorité belge de protection des données a rappelé que le contrôle incombe aux parties et que celles-ci « ne sont pas libres de déléguer » ni « d'abdiquer de celui-ci [. .]au nom d'un accord conjoint »[107].

Nous acceptons les conseils en la matière fournis par Bird & Bird et par l'APD et dès le mois de janvier nous avons signalé que « la poursuite des délibérations autour d'un modèle entièrement centralisé ne ferait que nous distraire, et retarder et rendre plus

[106] Phil Bradley-Schmieg & Ruth Boardman (Bird & Bird LLP), « Questions 1 et 2 : Responsabilité, garanties, autorité de contrôle et traiteur », 9 septembre 2019, page 6, 2.18.
[107] Autorité de protection des données (Belgique), Lettre à Goran Marby, le 4 décembre 2019, page 3, disponible ici.

coûteux l'accomplissement de notre mandat »[108]. Nous regrettons qu'en cette étape avancée de l'EPDP les propositions en vue de centraliser certaines décisions sur les données à caractère personnel des titulaires de noms de domaine et l'assignation de leur contrôle à travers nos recommandations de politiques soient encore de mise. [109]

Rien n'a changé depuis que l'EPDP a décidé de rejeter la centralisation, celle-ci ne permettant pas d'amoindrir la responsabilité des parties contractantes. [110] Certaines parties semblent ainsi soit ne pas comprendre, soit ignorer sciemment les conseils juridiques n'allant pas dans le sens des résultats politiques de leur choix. Dans les deux cas de figure, cela complique l'obtention d'un consensus autour des recommandations de mise en œuvre de politiques.

Le terme « centralisation » lui-même s'éloigne de ce que les défenseurs de ce modèle ont réellement proposé. La discussion sur un modèle « centralisé » portait sur la prise de décisions et non sur les données en tant que telles. Sans la possession des données sous-jacentes, il n'existe pas de modèle « centralisé » limitant le traitement de données inutiles, ou renforçant la sécurité des personnes concernées. Au contraire, ce genre de système ajoute des étapes de traitement supplémentaires inutiles et va à l'encontre des principes de base visant à définir par défaut la minimisation des données et le respect de la vie privée.

L'insistance pour dire que la « centralisation » de la divulgation de données à caractère personnel serait licite ou réalisable au sein de l'écosystème ICANN, alors même que cette option a déjà été rejetée, nous préoccupe. Bien que nous appuyions les efforts de l'ICANN pour résoudre la répartition de la responsabilité au sein d'un système centralisé, rien ne semble indiquer que ce transfert de responsabilité puisse être viable du point de vue juridique.

Comité permanent de la GNSO

Le RySG défend l'idée d'un SSAD qui soit flexible et à même de s'adapter en fonction de l'évolution du contexte pratique ou juridique. Nous reconnaissons que le SSAD doit

[108] Prochaines étapes de la CPH, lettre datée du 7 janvier 2020.

[109] Consulter notamment, les commentaires de catégorie 2 sur la Recommandation 9 de l'IPC/BC de juillet 2020 proposant « un processus non automatique de prise de décision centralisé au niveau du CGM » en dépit des conseils juridiques et de l'accord visant un modèle hybride : « En vertu des orientations juridiques reçues, l'équipe responsable de l'EPDP recommande que les types de requêtes suivantes, lorsqu'elles font l'objet d'un traitement et examen manuel, soient autorisées au titre du RGPD pour évaluer la méthode de divulgation (saisie et traitement de la décision de divulgation) par le gestionnaire d'entrée centralisé.
Décisions de divulgation automatique pour les requêtes portant clairement sur les « domaines correspondants à une marque déposée ».
Décisions de divulgation automatiques pour les requêtes portant clairement sur des cas d'hameçonnage.
L'ICANN est l'autorité de contrôle chargée du traitement de cette décision de divulgation.

[110] « Cela signifie donc que pour obtenir tout modèle d'accès unifié il faut soit parvenir à un accord sur les risques en responsabilité au niveau des 2500 parties contractantes, soit faire passer une motion [sic] afin d'alléger leur responsabilité juridique ». Goran Marby, transcription de la réunion en personne de l'EPDP du 25 septembre 2018, page 2, disponible ici.

être un système malléable, capable de s'adapter à un contexte en permanente évolution à cause des nouvelles directives administratives, décisions de justice et règlementations émanant de diverses juridictions. Cependant, nous rejetons l'idée selon laquelle les travaux du Comité permanent de la GNSO doivent avoir un résultat prédéterminé. Tout particulièrement, nous ne pouvons accepter l'idée selon laquelle le SSAD devrait, inévitablement, évoluer vers davantage de centralisation et d'automatisation des divulgations de données personnelles à l'avenir. L'évolution du SSAD doit reposer sur des faits et des données et non sur des conjectures ou présomptions.

Tel que nous l'avons déjà mentionné, le modèle hybride reflète ce qui est actuellement possible du point de vue juridique. Notre accord pour un modèle hybride ne repose pas sur l'idée qu'il devienne par la suite un modèle centralisé car nul ne peut savoir comment vont évoluer les lois. Nous acceptons le modèle hybride comme une solution pour sortir du statut quo tout en préservant adéquatement les données à caractère personnel individuelles.

Les membres du groupe de travail consacré à l'EPDP devraient offrir des attentes réalistes sur la façon dont le SSAD peut évoluer au cours du temps aux membres de leur groupe. Bien que pouvant évoluer dans la direction souhaitée par certains des membres de l'EPDP, il est également probable, voire plus, que le système devienne à l'avenir plus restrictif, moins automatique ou plus décentralisé. [111] Le fait de prédire que ce système évoluera en direction unique plutôt qu'en réagissant aux évènements et aux données le condamne d'avance à échouer aux yeux de certains membres de la communauté.

Dans le même sens, bien qu'ayant généralement appuyé la portée des travaux du Comité permanent de la GNSO, nous sommes préoccupés de voir que ce mécanisme se structure autour du renoncement à nos obligations juridiques en tant qu'autorité de contrôle. Ne pouvant anticiper la forme des futures orientations en la matière, nous nous sommes bien gardés d'affirmer catégoriquement que certaines modifications, tel que le fait d'automatiser les nouveaux cas d'utilisation, représentent une mise en œuvre plus qu'une politique. A moins que la Commission européenne ne fournisse des orientations précises, définitives et incontestables sur chaque thème, les propositions d'automatisation basées sur de nouvelles orientations seront certainement porteuses de risques résiduels, d'obligations supplémentaires ou exigeront, de la part des parties contractantes ou du gestionnaire de la passerelle centrale (CGM), des révisions contractuelles.

[111] Les principales décisions et orientations récentes dans ce domaine évoquent des applications et des restrictions de lois futures plutôt qu'un assouplissement des critères. *A titre d'exemple*, *consulter* l'affaire C-311/18 Commissaire à la protection des données versus Facebook Ireland Limited et Maximillian Schrems (« Schrems II ») invalidant le système de protection de la vie privée EU/U.S.A. ; *consulter également :* Communication de la Commission européenne au Parlement et au Conseil européens datée du 24 juin 2020 réclamant une application du RGPD renforcée plutôt que l'assouplissement des restrictions, disponible ici.

Il est probable que des directives nouvelles, même claires et permissives, sur une automatisation supplémentaire entraîneront des changements de politique. Ainsi, de nouvelles directives peuvent autoriser l'automatisation totale à partir du moment ou l'entité chargée du traitement des données dispose d'un délégué à la protection des données tel que le définit le RGPD. En l'état actuel, nos recommandations n'exigent pas aux parties (CGM, autorité en charge de l'accréditation, registre, bureau d'enregistrement, requérant) de disposer d'un délégué à la protection des données. D'après ce scénario, la mise en œuvre qui exige aux parties contractantes de procéder à davantage d'automatisation des cas d'utilisation entraînera davantage de risques juridiques si les parties ne disposent pas d'un délégué à la protection des données.

Cet exemple illustre bien l'importance de ne pas définir d'emblée si les changements impliquant des risques juridiques relèvent d'une mise en œuvre ou d'une politique. En tant qu'autorité de contrôle, nous demandons à rester réactifs face aux obligations qui sont les nôtres au regard des données à caractère personnel que nous traitons.

L'automatisation totale n'est possible que dans des contextes limités

Le RySG défend l'automatisation lorsque celle-ci est « viable du point de vue technique et commercial et permise par la loi ».[112] Ces critères constituent selon nous des sauvegardes garantissant que les personnes concernées ne fassent pas l'objet d'un traitement automatique abusif de leurs données.

Il est évident que l'automatisation de décisions ayant des répercussions sur les personnes concernées - et dont elles ne tirent aucun avantage- ne se fait généralement pas dans l'intérêt de celles-ci. Tel que le RGPD le stipule, « les personnes concernées doivent avoir le droit de ne pas faire l'objet de décisions reposant uniquement sur un traitement automatisé, y compris le profilage, et ayant sur elles des effets juridiques ».[113] Bird &Bird nous a confirmé que parmi les cas d'utilisation pouvant être soumis à l'automatisation, seuls quatre d'entre eux sont sans effets juridiques ou tout aussi significatives pour les personnes concernées. [114]

Nous pouvons conclure de cet avis juridique que seuls de rares ensembles de décisions sont sans effet juridique ou d'un autre ordre pour les personnes concernées. La note ne fait pourtant qu'évaluer ces cas d'utilisation au regard du RGPD. Nous devons donc être prudents avant de conclure trop largement quant à leur licéité qui entraîne les parties

[112] Rapport final de l'étape 2 de l'EPDP, 9.3.

[113] Article 22 du RGPD.

[114] Rapport final de l'étape 2 de l'EPDP, 9.4. (i) des requêtes des autorités d'application de la loi des juridictions locales ou autres juridictions concernées avec soit 1) un fondement juridique avéré au titre du RGPD 6(1)e ou 2) le traitement doit se faire au titre d'une exemption de l'article 2 du RGPD ; (ii) l'enquête sur une violation présumée de la législation en matière de protection des données commise par l'ICANN ou les parties contractantes affectant le bureau d'enregistrement ou l'autorité de protection des données ; (iii) une requête concernant uniquement le champ « ville » afin d'évaluer le dépôt d'une plainte ou à des fins statistiques ; (iv) l'absence de données à caractère personnel dans les registres divulgués précédemment par les parties contractantes.

contractantes à mettre en œuvre des conditions qui ne feront qu'augmenter le risque juridique auquel elles sont soumises.

Nous sommes aussi inquiets de voir que ces quatre cas d'utilisation seront désormais traités d'emblée automatiquement par le SSAD[115], malgré le fait que l'équipe responsable de l'EPDP n'ait pas encore entamé les discussions techniques sur la façon dont un algorithme peut fiablement (i) identifier les requêtes susceptibles d'être correctement automatisées, ou (ii) prendre des décisions de façon fiable, exacte et transparente. En assemblée plénière nous avons accordé que l'automatisation devait respecter trois critères : (i) la viabilité technique, (ii) la viabilité commerciale, et (iii) la licéité.[116] En demandant d'automatiser les cas d'utilisation au point 9.4 sur la base de leur licéité, nous avons fusionné ces trois sauvegardes majeures en une évaluation unique de la légalité pour ces cas d'utilisation ;

En effet, la seule approche suivie pour évaluer comment un algorithme pourrait prendre ce type de décision envisage que le CGM fournisse des recommandations portant sur la divulgation aux parties contractantes, l'algorithme apprenant grâce aux retours provenant de la comparaison des décisions de divulgation d'une partie contractante avec les recommandations automatiques.[117] Au-delà d'une méconnaissance totale du fonctionnement général du *machine learning,* la fiabilité des recommandations émises par un système ne disposant pas des informations sous-jacentes à ces décisions nous pose question. Même si des correspondances peuvent s'établir entre les décisions prises et les décisions automatisées, cette corrélation n'implique pas que l'algorithme prenne des décisions fiables.

Il faut une approche plus fine du *machine learning* et de l'apprentissage algorithmique pour évaluer si ces cas d'utilisation sont techniquement viables. D'où l'importance de la faisabilité technique comme facteur indépendant à considérer dans l'automatisation des cas d'utilisation. Si les parties devant à présent définir la faisabilité technique et construire l'algorithme échouaient, nous ne devrions pas nous laisser bloquer par l'automatisation obligatoire tant que sa viabilité technique n'ait pas été atteinte.

La viabilité financière exige notre attention

Dès le début de l'étape 2, le RySG a plaidé en faveur d'une évaluation financière du SSAD proposé afin de guider les prises de décisions de l'équipe responsable de l'EPDP. Nous apprécions le travail réalisé par l'équipe de l'ICANN en vue de fournir une évaluation des coûts. Au regard des coûts de développement et d'entretien du SSAD proposé estimés par l'ICANN, nous nous inquiétons de voir cette évaluation reléguée

[115] Rapport final de l'EPDP, 9.4. « En vertu de l'orientation juridique reçue [. . .] l'équipe responsable de l'EPDP recommande que les types de requêtes de divulgation suivantes, désignées aptes du point de vue juridique à l'automatisation totale au titre du RGPD (saisie et traitement des décisions de divulgation) DOIVENT être automatisées dès le lancement du SSAD. . . »
[116] Rapport final de l'étape 2 de l'EPDP, 9.3.
[117] Rapport final de l'étape 2 de l'EPDP, 5.1.1, 5.5

en note de bas de page dans le rapport final tandis que certaines unités constitutives continuent à repousser le principe que les utilisateurs du SSAD assument les coûts opérationnels du système.

Nous revenons sur un point que nous avons souvent évoqué lors des délibérations. Les personnes concernées ne doivent en aucun cas subventionner le fait qu'un tiers accède à leurs données personnelles. Le SSAD qui a pour but d'offrir un accès aux données normalisé et prévisible doit être financé par ceux qui tirent directement parti d'un tel service.

En outre, nous appuyons la démarche de l'ICANN de procéder à une analyse du rapport coûts-bénéfices afin de déterminer la viabilité financière d'un tel système. Grâce à l'ampleur des travaux réalisés par l'étape 1 pour établir un processus normalisé permettant à un tiers de requérir directement des données auprès des parties contractées (Recommandation 18), toute partie (personne concernée ou requérant tiers) dispose à présent d'un processus prévisible pour requérir des données à caractère personnel. En outre, tout utilisateur qui ne souhaiterait pas payer le service du SSAD peut choisir l'option d'une requête de divulgation, comme établit par l'étape 1, sans coûts pour le requérant.

Selon nous, l'absence d'analyse coût-bénéfice entraîne d'autres écueils plus graves : l'EPDP n'est jamais parvenu à établir – au-delà des conjectures et anecdotes - quel était le problème réel qu'il était censé remédier. Nous n'avons vu aucune donnée fiable faisant état d'un quelconque problème dans les réponses fournies par les parties contractantes aux requêtes de divulgation. Les données semblent plutôt indiquer que la plupart des requêtes bien formulées obtiennent une réponse et que l'absence de celle-ci tient généralement à (i) une requête ne respectant pas la protection des données/vie privée, ou (ii) l'absence de réponse des requérants lorsqu'une information supplémentaire est requise. [118] Le SSAD n'offre aucune solution pour ces erreurs de la part du requérant.

Les questions de priorité 2 ont été abordées

Bien que le RySG soit en faveur de travaux supplémentaires sur les questions de priorité 2 telles que l'exactitude, la distinction entre personne physique et morale et la faisabilité des contacts uniques, nous ne sommes pas d'accord pour dire que ces questions n'ont pas été abordées lors de l'étape 2. De fait, chacune d'entre elles a été largement abordée, notamment à travers les analyses détaillées fournies par Bird & Bird en faveur du maintien du statut quo. Nous recommandons que les travaux futurs ne partent pas de zéro mais s'appuient sur le travail de taille réalisé par l'équipe responsable de l'EPDP sur ces thèmes La transparence et l'exactitude à l'heure de nous

[118] *Consulter :* Vie privée et accès légal et Vie privée et accès légal aux données à caractère personnel à Tucows, 13 mars 2020, disponible ici.

prononcer sur ces sujets nous semblent essentielles pour éviter des malentendus dans la communauté. Par exemple :

Exactitude - Bird & Bird a confirmé qu'aux termes du RGPD l'exactitude constitue un droit des personnes concernées (et non des tiers) et une obligation pour les autorités de contrôle des données.[119] En outre, Bird & Bird a confirmé que les procédures existantes dans le cadre du contrat d'accréditation de bureau d'enregistrement visant à confirmer les données des titulaires de noms de domaine ne suffisent pas à remplir les critères d'exactitude aux termes du RGPD. [120]

Distinction entre personne morale et personne physique - Nous ne contestons pas le fait que le RGPD s'applique aux données des personnes physiques et non des personnes morales. Nous avons souligné que l'enjeu pratique était de déterminer de façon fiable de quel cas de figure il s'agissait et de gérer les registres des personnes morales pouvant contenir des données sur des personnes physiques. Tandis que certains ont proposé de recourir au mécanisme du consensus pour réduire le risque, Bird & Bird confirme la complexité de cette solution et le fait qu'elle n'élimine pas les risques de responsabilité pesant sur les parties contractantes. [121]

Faisabilité des contacts uniques - Nous avons reçu une orientation juridique précise sur ce thème faisant état du fait que bien que l'anonymisation et la pseudonymisation s'avéraient être des mesures utiles pour renforcer la protection de la vie privée, la publication de courriers électroniques masqués ne remplissait pas ce critère, le but de ceux-ci étant justement de permettre que les personnes soient contactées.[122] En outre, nous remarquons que bien que la formulation de la recommandation sur cette question proposée à la plénière du 12 mars 2020 n'ait pas reçu d'objection, elle ne figure pas dans le rapport final.[123]

Les autorités de contrôle ont besoin de flexibilité pour s'acquitter de leurs obligations

[119] Ruth Boardman & Katerina Tassi (Bird & Bird LLP), « Avis sur le principe d'exactitude au titre du Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD ») : enquêtes de suivi sur les notes concernant la « distinction entre personne morale et personne physique » et « exactitude », datées du 9 avril 2020.
[120] Ruth Boardman & Gabe Maldoff (Bird & Bird LLP), « Avis sur le principe de l'exactitude au titre du Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD ») » daté du 8 février 2019.
[121] Ruth Boardman (Bird & Bird LLP), « Avis sur les options de consentement en vue de rendre publiques les données à caractère personnel dans le RDS et exigences au titre du Règlement général sur la protection des données (Règlement (UE) 2016/679) (« RGPD »), » daté de mars 2020.
[122] Ruth Boardman (Bird & Bird LLP), « "Lot 2" de questions à propos du RGPD portant sur un système normalisé d'accès et de divulgation (« SSAD »), enregistrement fiduciaire ou anonymisé et adresses de courrier électronique pseudonymisées », daté du 4 février 2020.
[123] « L'équipe responsable de l'EPDP a accepté le texte de la recommandation préliminaire aussi bien pour la faisabilité des contacts uniques que pour avoir une adresse e-mail anonymisée uniforme et l'expurgation du champ « ville ». Le soutien du personnel inclura cette recommandation préliminaire dans le supplément aux sujets de priorité 2 qui seront publiés pour consultation publique. Email de Caitlin Tubergen à l'équipe EPDP-GNSO daté du 12 mars 2020.

Bien que nous appuyions les compromis nécessaires pour parvenir à un accord sur la Recommandation 8 (Autorisation des parties contractantes) nous craignons que le cadre ne soit devenu trop prescriptif. Les directives de départ sur la façon dont les entités chargées de la divulgation POURRAIENT décider sont devenues un cadre rigide régissant la façon dont elles DOIVENT prendre les décisions. Bien que les opérateurs de registre soutiennent le principe de la normalisation établi par le groupe de travail, cette politique ne peut aucunement rendre compte de tous les cas de figure de lois et règlements en matière de vie privée des différentes juridictions locales, notamment lorsque qu'il s'agit de requêtes transfrontalières. Nous devons porter une attention particulière à la mise en œuvre et à l'application de cette recommandation pour laisser aux entités chargées de la divulgation suffisamment de flexibilité pour s'acquitter de leurs obligations spécifiques au niveau juridique et juridictionnel et éviter ainsi que cette recommandation ne soit jugée inapplicable.

Finalité 2

La nouvelle formulation de la finalité de la Recommandation 22 substitue la finalité 2 originale de la Recommandation 1 de l'étape 1 de l'EPDP, laquelle n'a fait l'objet ni d'un accord ni d'une adoption de la part du Conseil d'administration de l'ICANN. Nous réaffirmons nos préoccupations déjà présentes lors de l'étape 1[124], face à cette finalité qui n'en constitue pas une au sens juridique du terme, tel que défini dans le RGPD.[125] La formulation « contribuer au maintien de la sécurité, la stabilité et la résilience du système des noms de domaine, conformément à la mission de l'ICANN » ne laisse pas clairement entendre aux personnes concernées la façon dont leurs données seront traitées ni les raisons de le faire. Ceci étant dit, face au soutien du Conseil d'administration porté à cette finalité [126]et de l'esprit ayant présidé à sa conception, le RySG a accepté de ne pas s'y opposer.

Conclusion

Le RySG s'est engagé à participer activement et avec bonne foi à l'élaboration de recommandations de politiques de consensus adaptées à l'accès aux données des titulaires de noms de domaine. Nous avons veillé à ce que ces recommandations tracent une voie claire, dans le respect du RGPD, qu'elles soient raisonnables du point de vue commercial et applicables, qu'elles prennent en compte nos différents modèles

[124] Rapport final de l'étape 1 de l'EPDP, Déclaration minoritaire du RySG au sujet de l'étape 1, page 166, disponible ici.

[125] Orientations de l'ICO sur la limitation des finalités : « Cette condition vise à garantir que les raisons pour lesquelles vous souhaitez obtenir des données à caractère personnel soient claires et transparentes, et que l'usage que vous en ferez s'accorde avec les attentes raisonnables que peuvent avoir les personnes concernées. Le fait de préciser votre finalité dès le départ vous permet d'être plus redevable tout au long de votre processus et d'éviter les usages détournés. Cela permet également aux individus de mieux comprendre la façon dont vous utilisez leurs données, de décider s'ils souhaitent ou non partager ces renseignements et d'affirmer leurs droits sur leurs données, le cas échéant. Il est essentiel de renforcer la confiance publique quant à l'usage que nous faisons des données à caractère personnel. Disponible ici.

[126] Lettre de Maarten Botterman à Keith Drazek, datée du 11 mars 2020, disponible ici.

commerciaux et n’entravent pas l’innovation. Sur la base de ces principes et en prenant note des préoccupations suscitées, nous avons accordé notre soutien consensuel aux recommandations du rapport final. Nous attendons avec intérêt leur considération plus approfondie et leur approbation par le conseil de la GNSO.

SSAC : Déclaration minoritaire sur le rapport final portant de l'étape 2 du processus accéléré d'élaboration de politiques (EPDP) sur la spécification temporaire relative aux données d'enregistrement des gTLD - SSAC 112

Préface

Déclaration minoritaire du Comité consultatif sur la sécurité et la stabilité de l'ICANN (SSAC) portant sur le rapport final de l'étape 2 du processus accéléré d'élaboration de politiques (EPDP) sur la spécification temporaire relative aux données d'enregistrement des gTLD.

Le SSAC s'occupe des questions liées à la sécurité et la stabilité des systèmes de nommage et d'allocation d'adresses Internet. Ceci inclut des questions opérationnelles (par exemple se rapportant à l'opération correcte et fiable du système de publication de la zone racine), des questions administratives (par exemple se rapportant à l'affectation d'adresses et à l'attribution de numéros sur Internet), et des questions liées à l'enregistrement (par exemple se rapportant aux services des registres et des bureaux d'enregistrement). Le SSAC se livre à une évaluation continue des menaces et à une analyse des risques des services de nommage et d'attribution d'adresses Internet pour évaluer les principales menaces à la sécurité et à la stabilité, et conseiller la communauté de l'ICANN en conséquence. Le SSAC n'a pas d'autorité pour réglementer, faire valoir ou se prononcer. Ces fonctions sont du ressort d'autres services, et l'avis donné ici devrait être évalué selon ses propres mérites.

Résumé analytique

Le SSAC ne peut pas approuver le rapport final portant sur l'étape 2 du processus accéléré d'élaboration de politiques sur la spécification temporaire relative aux données d'enregistrement des gTLD [127](dorénavant « le rapport final ») en l'état actuel.

En premier lieu, nous considérons qu'un système bien meilleur serait envisageable dans le cadre des limites imposées par le Règlement général sur la protection des données (RGPD) et que l'EPDP *n*'est *pas* parvenu à fournir des résultats qui soient aptes pour la sécurité et la stabilité.

Deuxièmement, dans ses recommandations le rapport final ne mentionne pas l'engagement d'achever les points de la charte n'ayant pas été abordés. Le SSAC a conditionné sa participation et son soutien à l'étape 2 de l'EPDP à l'engagement que soient examinées plusieurs questions de l'étape 1. Malheureusement celles-ci n'ont pas été examinées et restent sans réponse.

[127] Consulter https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-31jul20-en.pdf.

Troisièmement, en marge des questions abordées ci-dessus, le SSAC objecte certaines recommandations spécifiques qui demeurent, à savoir :

- *Recommandation 6 : Niveaux de priorité.* Le classement des menaces de cybersécurité comme « priorité 3 » ne suffit pas à contrer ces graves menaces en ligne.
- *Recommandation 10 : Détermination de conventions de service (SLA) variables relatives aux délais de réponse du SSAD.* Le SSAC s'inquiète du temps de réponse trop élevé, du fait que les SLA ne soient pas applicables dans les faits et que les avis relatifs à la mise en œuvre risquent de prolonger progressivement le temps de réponse des parties contractantes.
- *Recommandation 12 : Obligation de divulgation.* Le SSAC craint que les parties contractantes puissent, à leur discrétion, révéler l'identité des requérants de données au lieu de ne le faire que lorsque la loi en matière de protection des données l'exige. La divulgation de l'identité des requérants peut s'avérer dangereuse pour eux comme pour leurs enquêtes.
- *Recommandation 14 : Viabilité financière.* D'après le libellé de la recommandation, les frais sont transférés aux victimes, ce qui contrevient aux pratiques commerciales habituelles et va à l'encontre des avis précédents du SSAC au Conseil d'administration de l'ICANN. La recommandation, rédigée sans avoir suivi les procédures de la GNSO, ne repose sur aucun élément de preuves et risque de ne pas être conforme au RGPD.

Le système normalisé d'accès et de divulgation aux données d'enregistrement non publiques (SSAD) tel qu'il a été prévu dans l'étape 2 peut améliorer le statut quo si certaines recommandations sont modifiées et si la GNSO s'engage à achever les travaux prévus dans la charte de l'EPDP encore en suspens. Si la GNSO garantit que les questions liées à la distinction entre les personnes morales et physiques, à l'anonymisation et l'enregistrement fiduciaire et à l'exactitude des données seront examinées prochainement dans le cadre d'élaboration de politiques formelles, le SSAC serait disposé à approuver le rapport final.

1 Introduction

En participant à l'EPDP, le SSAC a fait preuve de professionnalisme et de bonne foi, consacrant bénévolement des milliers d'heures tout au long des deux étapes et travaillant avec assiduité auprès de nos collègues de la communauté de l'ICANN.

Comme déclaré dans le SAC111 :

> Comme la plupart des participants, le SSAC a accepté des compromis sur différents sujets pour pouvoir avancer en vue d'un système en ligne. Afin d'éviter toute confusion, le rapport de l'étape 2 et les recommandations qu'il

> préconise sont loin de ce que le SSAC considère comme des solutions possibles et nécessaires en matière de sécurité et de stabilité, dont la responsabilité incombe à l'ICANN. Le SSAC estime que la version initiale du Système normalisé d'accès et de divulgation (SSAD) ne sera pas à même de délivrer à temps et de façon appropriée les données pouvant satisfaire les besoins de sécurité opérationnelle variés. Nous considérons qu'il est possible d'obtenir un système plus approprié et respectueux des limites imposées par le RGPD. Afin d'avancer, au lieu de rester à attendre un système idéal, le SSAC approuve l'établissement de bases solides pouvant être améliorées en temps voulu.[128]

Le SSAC soutient la déclaration. Nous ne pouvons pas appuyer l'ensemble des résultats de l'étape 2 en leur état actuel.

Le SSAC estime qu'un meilleur système est possible dans le respect des limites imposées par le RGPD et que l'EPDP n'a pas fourni de résultats appropriés en termes de sécurité et de stabilité. En outre, dans ses recommandations le rapport final ne mentionne pas son engagement d'achever les points de la charte étant restés en suspens. Le SSAC avait conditionné sa participation et son soutien à l'étape 2 de l'EPDP à la promesse que plusieurs questions de l'étape 1 seraient examinées. Malheureusement celles-ci n'ont pas été examinées et restent sans réponse.

Parmi les vingt-deux recommandations du rapport final, le SSAC en rejette 4, à savoir :

- *Recommandation 6 : Niveaux de priorité.* Le classement des menaces de cybersécurité comme « priorité 3 » ne suffit pas à contrer ces graves menaces en ligne.
- *Recommandation 10 : Détermination de conventions de service (SLA) variables relatives aux délais de réponse du SSAD.* Le SSAC s'inquiète du temps de réponse trop élevé, du fait que les SLA ne soient pas applicables dans les faits et que les avis relatifs à la mise en œuvre risquent de prolonger progressivement le temps de réponse des parties contractantes.
- *Recommandation 12 : Obligation de divulgation.* Le SSAC craint que les parties contractantes puissent, à leur discrétion, révéler l'identité des requérants de données au lieu de ne le faire que lorsque la loi en matière de protection des données l'exige. La divulgation de l'identité des requérants peut s'avérer dangereuse pour eux comme pour leurs enquêtes.
- *Recommandation 14 : Viabilité financière.* D'après le libellé de la recommandation, les frais sont transférés aux victimes, ce qui contrevient aux pratiques commerciales habituelles et va à l'encontre des avis précédents du SSAC au Conseil d'administration de l'ICANN. La recommandation, rédigée sans

[128] Consulter le document SAC111, page 5 : https://www.icann.org/en/system/files/files/sac-111-en.pdf.

avoir suivi les procédures de la GNSO, ne repose sur aucun élément de preuves et risque de ne pas être conforme au RGPD.

Nous ne nous opposons pas au reste des recommandations du rapport final. Ce qui ne veut pas pour autant dire que nous en soyons heureux. A titre d'exemple, le SSAC soutient l'idée d'accréditation du SSAD car elle constitue une garantie conçue pour satisfaire le RGPD, pour permettre la confiance et documenter les requêtes légitimes. Toutefois, nous ne pouvons être certains que l'accréditation soit un instrument efficace. En vertu de la politique proposée, la divulgation des données reposera entièrement sur le processus de décision de chaque bureau d'enregistrement et opérateur de registre dont les méthodes et les normes d'évaluation peuvent varier énormément, entraînant ainsi des résultats inégaux, subjectifs et imprévisibles. La politique proposée ne fournira peut-être pas de recours efficace aux requérants de données qui risquent de se voir refuser des requêtes manifestement légitimes. Ainsi, malgré la force du programme d'accréditation déployé, celui-ci risque de ne pas donner de résultats et de ne pas justifier les gros efforts consentis par les requérants. Ce résultat, peu fiable, reste en deçà de ce que le RGPD autorise. [129]

Diverses recommandations du rapport final n'ont pu obtenir de consensus et ont reçu une opposition formelle de la part d'un grand nombre d'instances participant au processus. Toutefois, certains membres de la communauté réclament au conseil de la GNSO un vote selon une approche descendante de l'ensemble du rapport final, pour approuver l'ensemble des recommandations ou les rejeter en bloc. Nous estimons que cette approche en « tout ou rien » contournerait le processus consensuel. Cela violerait également la procédure de la GNSO selon laquelle « dans l'éventualité où le rapport final inclut des recommandations n'obtenant pas le consensus parmi l'équipe du PDP, le conseil de la GNSO devra délibérer pour décider de l'adoption ou du renvoi des recommandations en vue de futures analyses et travaux. [130]

Nous remarquons que bien que les recommandations visent à créer un programme général, elles ne sont pas suffisamment interdépendantes pour justifier un vote selon une approche en « tout ou rien ». Il est certainement possible de modifier certaines recommandations. Il est possible de rejeter certaines recommandations (et notamment certaines sous-recommandations) tout en conservant le reste tel quel. L'idée selon laquelle l'ensemble des efforts seraient réduits à néant si toutes les recommandations

[129] En juillet 2018, le Comité européen de la protection des données a écrit à l'ICANN en affirmant que « les données à caractère personnel traitées dans le cadre du WHOIS doivent être mises à disposition des tiers ayant un intérêt légitime à avoir accès à ces données, des garanties devant être mise en place pour assurer que la divulgation soit équilibrée et limitée au strict nécessaire et que les autres conditions du RGPD soient remplies... », Lettre du Comité européen de la protection des données à Göran Marby https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

[130] Guide de procédure de l'élaboration de politiques de la GNSO, chapitre 13 « Délibération du conseil », page 8. Cette procédure s'applique également aux EPDP. https://gnso.icann.org/sites/default/files/file/field-file-attach/annex-2-pdp-manual-24oct19-en.pdf

n'étaient pas acceptées, ou si elles ne le sont pas en l'état, est fausse. Selon les procédures de la GNSO « le conseil de la GNSO peut adopter l'ensemble ou une partie des recommandations contenues dans le rapport final et superviser les travaux de révision des recommandations ». Cela peut demander de gros efforts, mais c'est le devoir du conseil de la GNSO et du conseil d'administration de l'ICANN qui doivent également juger des résultats. La légitimité de l'ICANN et de son modèle multipartite se retrouvent de la sorte étudiée à la loupe.

Le reste de cette déclaration détaille des domaines clés qui préoccupent le SSAC.

2 Éléments de la charte non achevés

Dans le SAC111, le SSAC a exprimé sa préoccupation face aux éléments de la charte de l'EPDP n'ayant pas fait l'objet de discussions ni de décisions. Nous avons signalé que « des questions importantes impliquant les domaines de la distinction entre personnes morales et physiques, les services d'anonymisation et d'enregistrement fiduciaire et l'exactitude des données risquaient de ne pas être traités par l'EPDP »[131]. Ces thèmes en suspens dans l'étape 1 avaient été reportés. Le SSAC a conditionné sa participation et son soutien à l'étape 2 à l'engagement que ces questions seraient examinées. Malheureusement celles-ci n'ont pas été examinées et restent sans réponse. Par exemple,

- Les promesses d'examiner la distinction entre personnes physiques et personnes morales à travers le PDP ne figurent pas dans le rapport final.
- Le rapport final indique : « Conclusion - Exactitude et système de signalement de problèmes liés à l'exactitude du WHOIS : conformément aux instructions du conseil de la GNSO, l'équipe responsable de l'EPDP n'examinera pas ce sujet plus en détail ; plutôt, le conseil de la GNSO devrait former une équipe de détermination de la portée afin d'explorer davantage les problèmes liés à l'exactitude et l'ARS devrait aider à prendre une décision sur les prochaines étapes nécessaires pour traiter les problèmes potentiels identifiés ». Or, une équipe de détermination de la portée ne constitue pas une promesse de poursuite des travaux. Une prise de décision du niveau d'un PDP s'impose.
- Questions liées aux services d'anonymisation et d'enregistrement fiduciaire : Les travaux sur les questions liées à l'accréditation des services d'anonymisation et d'enregistrement fiduciaire (PPSAI) de 2016 n'ont pas répondu aux questions importantes posées par le RGPD alors qu'ils s'inscrivent dans le mandat de l'EPDP, de même que les pistes de travail de l'EDPD et du PPSAI se maintiennent cloisonnées. Des travaux supplémentaires sont nécessaires.

[131] SAC111 : consulter le commentaire du SSAC sur rapport initial du processus accéléré d'élaboration de politiques concernant la spécification temporaire relative aux données d'enregistrement des gTLD daté du 4 mai 2020, page 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

- Il est nécessaire de discuter de la façon dont les parties affectées peuvent demander des données de contact des domaines sous-jacents aux fournisseurs de services d'anonymisation et d'enregistrement fiduciaire accrédités par l'ICANN qui constituent des autorités de contrôle. Pouvoir demander ces données d'enregistrement est toute la raison d'être de l'EPDP et du SSAD. Le rapport final implique que l'ICANN laisse tous les domaines liés aux services d'anonymisation et d'enregistrement fiduciaire à l'extérieur du SSAD, de ses mécanismes de SLA et de reddition de comptes.
- Ceci figure dans la charte de l'EPDP. L'équipe de détermination de la portée et la mission de la charte de l'EPDP déclarent : « L'équipe responsable de l'EPDP examinera des recommandations accessoires qu'elle pourrait formuler en vue des travaux futurs de la GNSO éventuellement nécessaires pour garantir que les politiques de consensus pertinentes, y compris celles relatives aux données d'enregistrement, soient réévaluées de manière à devenir conformes aux lois applicables ».[132] Sur ce sujet, l'EPDP n'en a rien fait.

La question de la distinction entre les statuts des personnes morales et des personnes physiques n'a pas pu être résolue faute de recherches menées en temps voulu, sans qu'on en sache la raison. Le rapport de l'étape 1 de l'EPDP recommande à l'ICANN d'entreprendre « au plus vite » des recherches sur la faisabilité et les coûts d'une approche permettant de distinguer les statuts des personnes physiques et morales, la façon dont d'autres secteurs et organisations sont parvenus à le faire ainsi que les menaces pour la vie privée des titulaires de noms de domaine de distinguer ainsi les deux cas de figure (Recommandation 17.2).[133] Le 15 mai 2019, le Conseil d'administration de l'ICANN a approuvé cette recommandation et a chargé le personnel d'exécuter le projet comme contribution aux travaux de l'étape 2 de l'EPDP.[134]

Deux échecs sont à déplorer :

1. Le rapport de recherche a été restitué à l'EPDP le 8 juillet 2020, *après* l'élaboration du rapport final et donc trop tard pour permettre d'analyser

[132] Charte finale de l'EPDP adoptée – 19 juillet 2018, À consulter sur : https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter?preview=/88574674/90767676/EPDP%20FINAL%20Adopted%20Charter%20-%2019%20July%202018.pdf.

[133] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.

[134] Consulter la résolution du Conseil d'administration de l'ICANN du 15 mai 2019 https://features.icann.org/consideration-gnso-epdp-recommendations-temporary-specification-gtld-registration-data et la Recommandation 17, à la page 5 de la fiche de suivi du Conseil d'administration de l'ICANN qui l'accompagne, https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf

correctement la question de la distinction des statuts entre les personnes physiques et morales.

2. Le rapport de recherche ne s'est pas penché sur les exemples les plus parlants tel que la façon dont les données à caractère personnel des uns et des autres sont collectées, ou les raisons de le faire au sein des registres immobiliers, des registres commerciaux et des marques déposées au sein de l'UE ; le rapport n'explicite pas comment ce type de registres étrangers à l'UE gèrent les données des personnes vivant dans l'UE. Bien que le rapport affirme que « la plupart des opérateurs de ccTLD de l'Union européenne continuent de publier certains champs de données de contact (parfois tous) pour les domaines enregistrés par des personnes morales, [135], il ne fournit aucun détail, comme une liste répertoriant les ccTLD et les données publiées.

Le SSAC demande au conseil de la GNSO et au Conseil d'administration de l'ICANN de bien vouloir expliquer les raisons du retard de ce rapport et pourquoi le Conseil d'administration ne s'est pas acquitté de sa mission au nom des bénéficiaires visés : les membres de la communauté participant à l'EPDP. Afin d'éclairer des prises de décision futures, le rapport devra éventuellement être revu et complété par des analyses manquantes, mentionnées plus haut, et d'autres informations pertinentes.

Comme indiqué dans le SAC 111 : « La GNSO élabore des chartes pour permettre aux participants des groupes de travail de comprendre clairement les réalisations visées. La GNSO dispose de procédures et de normes applicables à ses groupes de travail élaborées pour faire avancer les travaux d'une façon prévisible et juste et les groupes prenant part à ces groupes de travail devraient être en mesure de tenir les engagements souscrits. L'échec de ces processus et les points essentiels qui n'ont pu être abordés remettent en question la légitimité de la façon dont l'ICANN élabore des politiques sur des questions d'intérêt mondial.[136]

3 Questions générales à considérer dans le cadre des priorités et de la réactivité aux requêtes

Ces deux recommandations sont intimement liées : la Recommandation 6 établit le principe de « priorité » des requêtes de divulgation de données tandis que la Recommandation 10 définit précisément la réactivité attendue par les parties contractantes. Les recommandations de politiques permettant de différentier les

[135] Différenciation des statuts des personnes physiques et morales dans les services d'annuaire des données d'enregistrement des noms de domaine. https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200708/5f72ece1/Rec17.2_Legal-Natural_8jul201-0001.pdf.

[136] SAC111 : Consulter le commentaire du SSAC sur rapport initial du processus accéléré d'élaboration de politiques concernant la spécification temporaire relative aux données d'enregistrement des gTLD daté du 4 mai 2020, page 8. https://www.icann.org/en/system/files/files/sac-111-en.pdf

priorités des divers types de requêtes de divulgation de données sont utiles puisque certaines données peuvent être urgentes pour remédier à des menaces pour lesquelles le temps joue ou du fait de l'ampleur de leurs conséquences, tandis que d'autres sont moins pressantes. Le fait de fournir des orientations politiques aux parties contractantes et à d'autres acteurs sur les procédures de divulgation et les délais de réponse (notamment le statut des requêtes et les données demandées) permet également d'aboutir à un système cohérent et transparent.

Malheureusement, les recommandations obtenues sont allées bien au-delà des recommandations de politique visées, allant jusqu'à prescrire une mise en œuvre détaillée de ces politiques. Ces spécifications rigides manquent de nuance et ne sont pas appropriées pour faire face à l'urgence d'accès aux données RDS, notamment dans le domaine de la cybersécurité. Malgré les bonnes intentions, la présence dans ces politiques d'un plan de mise en œuvre aussi détaillé risque d'induire un système trop complexe et difficile à gérer, surchargeant les parties contractantes pour certains types de requêtes et privant de réponse les requérants de données présentant des requêtes d'un autre type.

Le SSAC soutient les objectifs de haut niveau visant à créer un cadre pour les priorités et les attentes de réponse. Néanmoins, c'est à l'équipe responsable de la mise en œuvre de définir la manière d'organiser ses travaux. Cette équipe devrait inclure des représentants des parties contractantes fournissant les données demandées, les parties réalisant régulièrement des demandes de données, et le personnel de l'ICANN en charge de gérer et de superviser le SSAD. Les délais de réponse et les priorités peuvent être définis par cette équipe qui doit rendre compte des cas d'utilisation les plus courants et de leur urgence relative au vu des délais, des impacts et/ou autres facteurs accordés. Bien que n'étant pas exhaustive, la liste de la Recommandation 6.1.1 du rapport sur les demandes de priorité 1 peut constituer un point de départ pour ces discussions. Les recommandations finales de mise en œuvre de ce cadre doivent être examinées et approuvées par le conseil de la GNSO. Au fil du temps, ces facteurs pourraient être revus et adaptés par le biais des mécanismes évolutifs tel que l'envisage la Recommandation 18 ou tout équivalent adopté.

4 Objection à la Recommandation 6 sur les niveaux de priorité

En raison de son approche des questions de priorités et des SLA, tel que nous l'avons souligné plus haut, le SSAC rejette les Recommandations 6.1 et 6.2.

La classification des menaces de cybersécurité comme « priorité 3 » ne suffit pas à contrer les menaces en ligne actuelles. Ces classifications ne permettent pas de répondre à ces attaques en lignes qui demandent, de nos jours, des réponses flexibles. Ces dernières ont un impact financier avéré et exposent des millions de données personnelles sensibles en ligne, par exemple, des rançonlogiciels, des réseaux d'exfiltration de données et des extorsions par DDOS à une échelle massive. Ce

système de classification requiert des travaux supplémentaires pour analyser l'impact et la vitesse de ces différentes formes d'attaques. Ce système devrait tout au moins fournir un cadre politique permettant d'orienter les processus de mise en œuvre pratique pour gérer l'urgence des réponses en fonction de multiples facteurs. Une actualisation de la Recommandation 6 reconnaissant le besoin d'une réponse opportune face à la diversité des attaques et des limites plus strictes au niveau de la Recommandation 10 (détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD) sont nécessaires pour soutenir les réponses à ces attaques. Le SSAC a détaillé précédemment la raison d'être d'une telle approche dans le chapitre 3.2 du SAC 11[137].

5 Objection à la Recommandation 10 sur la détermination de la variable des conventions de service (SLA) relatives aux délais de réponse du SSAD

En raison de l'approche des questions de priorités et des SLA tel que nous l'avons souligné ci-dessus, le SSAC rejette la Recommandation 10. Bien que l'objectif de cette recommandation soit louable, le SSAC ne peut l'appuyer tel qu'elle est rédigée. Elle comporte des lacunes et n'offre pas de convention de service à même de répondre aux menaces de sécurité. Cela tient, entre autres, à la classification des menaces de sécurité comme « priorité 3 » dans la Recommandation 6 (Niveaux de priorité)[138]. Cette réponse est trop lente face à un incident de cybersécurité.[139]

L'objectif de la SLA de l'étape 1 est de 5 jours. Toutefois, il est indiqué dans le chapitre 10.11 : « Au cours de l'étape 2, les objectifs de conformité des parties contractantes pour les demandes de priorité 3 du SSAD seront de dix (10) jours ouvrables ». Il n'existe malheureusement aucune SLA contraignante dans l'étape 1 et ce n'est que dans l'étape 2 qu'est envisagée une SLA contraignante, assortie de pénalités. Malgré l'expérience acquise au fil du temps, la SLA de l'étape 2 autorise aux parties contractantes de répondre *plus lentement* que dans l'étape 1. Un délai de dix jours est bien trop strict en matière de stabilité et de sécurité. Depuis le rapport préliminaire, cette proposition n'a guère évolué. Or, le SSAC avait signalé à l'époque qu'il rejetait l'approche contradictoire de la section 3.2 du SAC111 :

> Ces objectifs ne concordent pas avec les raisons pour lesquelles le SSAD a été créé. Les demandes en matière de cybersécurité constituent habituellement une priorité élevée. Par nature elles sont opérationnelles et visent à empêcher de multiples victimes parmi le public lors des attaques (par exemple via des logiciels malveillants ou des activités d'hameçonnage). De même, les demandes opérationnelles de cybersécurité sont tout aussi urgentes que celles de l'URS.

[137] https://www.icann.org/en/system/files/files/sac-111-en.pdf

[138] Au-delà des cas de figure impliquant « une menace imminente sur la vie, des blessures graves, des menaces aux infrastructures critiques (en ligne et hors ligne) ou l'exploitation des enfants ».

[139] Seul un faible pourcentage de questions de sécurité et de cybercriminalité peut prétendre à une réponse de niveau 1 impliquant « une menace imminente sur la vie, des blessures graves, menaces aux infrastructures critiques (en ligne et hors ligne) ou d'exploitation des enfants ».

> En outre, le modèle général du SSAD considère que les demandes de cybersécurité seront faites par les parties accréditées, à travers un système transparent n'exigeant aucun examen approfondi. Le SSAC recommande que les demandes de sécurité opérationnelle (de la part des parties accréditées) soient reconnues de priorité 2. Si le volume des demandes de sécurité préoccupe les parties contractantes, un délai de réponse de trois (3) jours ouvrables serait raisonnable.
>
> Les requérants et les parties contractantes gagneront progressivement en confiance et en efficacité, le temps de réponse n'ayant donc aucune raison de s'allonger. Par conséquent, il n'est pas logique d'augmenter le temps de réponse des autorités de contrôle (comme le prévoit le SLA) entre l'étape 1 et l'étape 2 pour quelque niveau de priorité des requêtes que ce soit, le temps de réponse devant plutôt se maintenir ou diminuer pour les priorités de même niveau.

Le SSAC se préoccupe de voir que les SLA ne sont pas applicables dans les faits et que les conseils de mise en œuvre laissent à désirer. Le temps de réponse des SLA résulte de la moyenne de tous les temps de réponse. Une partie requérante peut cependant rejeter rapidement une requête de données ou demander d'emblée davantage d'informations. Cela entraînera donc un temps de réponse moyen très long pour les parties contractantes et permettra aux parties contractantes de repousser d'autres requêtes pour un laps de temps important avant de se retrouver à violer la SLA pertinente. Ces mesures automatiques ne sont pas interdites dans le cadre de la Recommandation 8.1. Il est donc essentiel que le département en charge des services de conformité de l'ICANN puisse vérifier si les parties contractantes sont en train d'examiner les demandes et ont bien répondu conformément à la Recommandation 8. Ne sachant pas comment le personnel de l'ICANN peut s'assurer de cela, nous ne savons pas comment les SLA peuvent être applicables concrètement.

6 Objection à la Recommandation 12 sur les conditions de divulgation

La Recommandation 12.2 autorise les parties contractantes à révéler l'identité des requérants de données lorsqu'elles le souhaitent, permettant ainsi de le faire de façon courante et automatique. Cette recommandation risque d'ignorer l'avis du Comité européen de la protection des données (CEPD) à l'ICANN qui indique qu'il n'est pas nécessaire de révéler aux personnes concernées (titulaires de noms de domaine) l'identité des requérants. La révélation de l'identité des requérants compromet les enquêtes, peut mettre en danger la sécurité et les droits de ceux-ci et risque de limiter les demandes au titre de l'article 6, ce qui ne représente certainement pas l'intention du RGPD. Les parties contractantes doivent réaliser des tests d'équilibrage avant de révéler l'identité des requérants, car les tiers requérants sont des personnes concernées et, à ce titre, bénéficient également de droits aux termes du RGPD.

La Recommandation 12 devrait interdire aux parties contractantes de révéler l'identité des requérants tant que la loi en vigueur ne l'*exige pas.* Nous recommandons aux autorités de contrôle de s'en tenir à la loi sans aller au-delà. Réaffirmant le SAC055 et le SAC101v2, « le SSAC estime que les autorités d'application de la loi et les responsables de la sécurité ont un besoin légitime d'accéder à l'identité réelle des parties impliquées derrière un nom de domaine. Cet accès doit se faire conformément aux exigences règlementaires.

Dans sa lettre datée du 10 mai 2018, l'ICANN a demandé au Comité européen de la protection des données (CEPD) :

> « a) Si l'identité de la personne/entité présentant une requête WHOIS doit être visible pour le titulaire de nom de domaine ou d'autres tiers.
>
> b) Si les requêtes des forces de l'ordre souhaitant accéder à des données WHOIS non-publiques doivent être visibles pour le titulaire de nom de domaine ou d'autres tiers ».

Dans sa réponse, le CEPD déclare :

> « L'assurance de la traçabilité de l'accès à travers des mécanismes de journalisation n'entraîne pas nécessairement une communication active (« push ») des informations journalisées [les identités des requérants] aux titulaires de noms de domaine ou d'autres tiers. Il incombe à l'ICANN et à d'autres autorités de contrôle de participer au système WHOIS afin de garantir que les informations d'enregistrement ne soient pas divulguées à des entités non-autorisées, afin notamment de ne pas mettre en danger les activités légitimes des autorités d'application de la loi ».[140]

Le RGPD exige aux autorités de contrôle, lorsqu'elles offrent leurs services, d'informer les personnes concernées quant aux *types* de parties pouvant traiter leurs données. Le RGPD ne demande pas de notifier activement les personnes concernées pour les informer que leurs données ont fait l'objet d'une requête. Le RGPD pourrait exiger aux autorités de contrôle de remettre l'identité des tiers requérants aux personnes concernées *si et seulement si les personnes concernées en font la demande.*

Le fait de révéler l'identité des requérants pose certains problèmes aux parties contractantes. Le fait de révéler l'identité des requérants nuit et limite le recours à l'article 6 du RGPD. Cela risque d'entraver l'accès à ces données ayant une finalité légitime au titre du RGPD - tel que l'atténuation de la cybercriminalité, la défense des victimes et les enquêtes en vue de procès ou pour faire appliquer la loi. Une exception demeure dans le RGPD en ce qui concerne les droits des personnes concernées à être informées, lorsque la révélation ou notification risque d'empêcher une partie (tel que

[140] Lettre d'Andrea Jelinek, présidente du CEPD, à Göran Marby Président-directeur général de l'ICANN du 5 juillet 2018. https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

le tiers requérant) d'atteindre ses finalités légitimes. [141] Comme dans le cadre d'une enquête, notamment. [142]

Ces questions n'ont pas été examinées par l'EPDP et celui-ci n'a pas reçu de conseil juridique approprié sur ces thèmes. Nous nous interrogeons sur les droits des requérants de données : ceux-ci étant des personnes concernées, leurs données se trouvent également protégées au titre du RGPD. Lors d'une requête au titre de l'article 6(1)(f), un requérant de données peut-il se voir forcé à renoncer à ses droits en matière de vie privée au profit de la personne concernée ou de l'autorité de contrôle ? (Le RGPD stipule qu'aucune personne concernée ne peut être forcée d'accepter la condition contractuelle de renoncer à ses droits en matière de vie privée). Ne serait-il pas juste que les parties contractantes annoncent à l'autorité de contrôle qu'elles ont partagé l'identité de cette dernière avec le titulaire de nom de domaine, notifiant ainsi les deux parties ?

Le SSAC a posé des questions sur ce thème à l'EPDP et à son équipe juridique, proposant que la question face l'objet d'un conseil juridique externe. L'EPDP a rejeté cette demande et les questions n'ont jamais été renvoyées à Bird & Bird. Il en résulte que l'EPDP, du fait de ne pas être pleinement informé, autorise des excès inutiles potentiellement dangereux.

7 Objection à la Recommandation 14 sur la viabilité financière

Le SSAC rejette les Recommandations 14.2 et 14.6

La formulation suivante de la Recommandation 14.2 s'avère inacceptable :

> L'objectif est que le SSAD puisse être financièrement auto-suffisant et n'entraîne pas de frais supplémentaires pour les titulaires de noms de domaine. Les personnes concernées NE DOIVENT PAS endosser les frais de divulgation des données aux tiers ; les personnes requérant des données du SSAD doivent assumer les coûts d'entretien du système en premier lieu ». En outre, les personnes concernées NE DOIVENT PAS endosser les frais du traitement des requêtes de divulgation des données qui ont été refusées par les parties contractantes suite à l'évaluation de la requête soumise par les utilisateurs du SSAD. L'ICANN POURRAIT contribuer à couvrir (partiellement) les frais d'entretien de la passerelle centrale. Pour plus de clarté, l'équipe responsable de l'EPDP considère que les titulaires de noms de domaine sont la source première d'une grande partie des revenus de l'ICANN. Ce revenu ne constitue

[141] Article 14 paragraphe 5 du RGPD

[142] Bureau du commissaire à l'information, « Droit à l'information : Existe-t-il des exceptions ? » https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#:~:text=There%20is%20no%20automatic%20exception,a%20specific%20exception%20or%20exemption.

pas en lui-même une violation à la restriction selon laquelle « [les personnes concernées NE DOIVENT PAS endosser les frais de divulgation de données à des tiers.

1) Les requérants de données ne devraient pas endosser les coûts associés à l'entretien du système en premier lieu.[143] Les requérants devraient certainement payer les frais d'accréditation et de conservation de leur accès au système. Toutefois, la formulation de la recommandation 14.2 fait que les victimes et les défenseurs se retrouvent à assumer les frais d'exploitation du système, ce qui est injuste et menace la sécurité de l'Internet. Tel que le SSAC l'a signalé dans le SAC101v2, « l'absence de gratuité du système [qui oblige les requérants à payer les frais de requête] risque de rendre la localisation et l'atténuation des abus de domaines très couteuses et difficiles du point de vue opérationnel ».

2) Cette formule trop large risque d'être mal interprétée : « les personnes concernées NE DOIVENT PAS endosser le coût de la divulgation des données à des tiers ». Cela a ensuite été modifié comme suit : « Pour plus de clarté, l'équipe responsable de l'EPDP considère que les titulaires de noms de domaine sont la source première d'une grande partie des revenus de l'ICANN. Ce revenu ne constitue pas en lui-même une violation à la restriction selon laquelle « les personnes concernées NE DOIVENT PAS endosser les frais de divulgation de données à un tiers ».

Ce libellé empêche toujours les bureaux d'enregistrement de transférer les coûts du programme SSAD aux titulaires de noms de domaine dans le cours normal des affaires. Habituellement, les parties contractantes considèrent l'essentiel de leurs coûts comme des coûts opérationnels et peuvent les transférer à leurs clients.[144] Cependant, la Recommandation 14.2 l'interdit. Aucun PDP n'a jamais protégé les titulaires de noms de domaine d'avoir à payer les coûts associés aux services d'enregistrement essentiels ou à la mise en œuvre de politiques de consensus. Aucun PDP antérieur n'a tenté de manipuler le fonctionnement des forces du marché tel que le propose la Recommandation 14.

Si l'objectif est simplement d'interdire aux bureaux d'enregistrement de faire payer des frais de service à un titulaire de nom de domaine lorsqu'un tiers demande ces données, affirmons-le haut et fort.

3) Le SSAD n'a pas l'obligation d'être « financièrement auto-suffisant » et les fondements de l'EPDP en ce sens sont insuffisants. Comme nous l'avons déjà affirmé, [145] le SSAC considère qu'il faut évaluer l'impact sur les utilisateurs et sur la sécurité et stabilité de la mise en place de frais d'accès au RDDS ou de toute autre modification majeure à l'avenir. L'EPDP n'a pas procédé à l'analyse de questions connexes tel que

[143] Consulter également la Recommandation 14.6.
[144] Consulter l'article 5.4. du SAC101v2.
[145] Consulter les documents SAC101v2 et SAC111.

demandé et n'a pas su justifier cette recommandation de politique tel que l'exige la procédure de la GNSO. La formulation à la Recommandation 14.2 ignore également l'avis du SSAC au Conseil d'administration de l'ICANN soumis à la GNSO. Tous ces facteurs rendent la Recommandation 14 prématurée.

Le 23 juin 2019, le Conseil d'administration de l'ICANN a analysé le SAC101v2 et a soumis ses recommandations au conseil de la GNSO pour considération de leur inclusion aux travaux de l'étape 2 de l'EPDP. L'avis stipule que : Dans le cadre d'un PDP formel, l'impact sur les utilisateurs et sur la sécurité et stabilité de la mise en place de frais d'accès au RDDS ou de toute autre modification majeure à l'avenir doivent être évalués. et : « Le Conseil d'administration de l'ICANN doit assurer une évaluation formelle des menaces de la politique relative à l'enregistrement des données afin de contribuer au processus d'élaboration de politiques. Il faut également conduire une autre évaluation des menaces de la mise en œuvre de la politique ». [146]

Ces évaluations d'impact sur les utilisateurs et sur la sécurité n'ont jamais été conduites nulle part. L'EPDP ne devrait pas allouer des frais aux requérants du SSAD sans avoir évalué au préalable leur impact sur ceux-ci et sur la sécurité du DNS.

L'EPDP n'ayant pas suivi les procédures de la GNSO lors de l'élaboration de la Recommandation 14.2, cette proposition de politique est sans fondement. Le manuel PDP de la GNSO stipule que : « L'équipe responsable du PDP évaluer soigneusement les impacts budgétaires, l'applicabilité ou la faisabilité des demandes d'informations qu'elle propose et de ses recommandations subséquentes ». Le manuel PDP de la GNSO exige également qu'« une déclaration portant sur les discussions du groupe de travail sur l'impact des recommandations proposées prenant en compte des domaines tels que l'économie, la concurrence, les activités, la vie privée et d'autres droits, l'évolution et la faisabilité » soit intégrée au rapport initial.

Cependant l'EPDP n'a pas procédé à l'évaluation des impacts budgétaires et de mise en œuvre *sur les requérants.* L'EPDP n'a pas procédé à l'évaluation des impacts budgétaires et de mise en œuvre en général, se contentant d'une estimation vague et non documentée sur les coûts de lancement du système central fournie par le personnel de l'organisation ICANN. L'EPDP n'a guère analysé les aspects liés à la concurrence et aux opérations, n'évaluant pas, non plus, la façon dont les frais d'accès auront un impact sur la sécurité et la stabilité. La formulation de la Recommandation 14.2 n'a pas été suffisamment étudiée ni justifiée.

Suite aux vastes déclarations de politique figurant dans la Recommandation 14.2, le rapport final déclare que tous les détails doivent être traités dans l'étape de mise en œuvre. Lors de l'étape de mise en œuvre, laquelle ne convient guère à l'analyse de

[146] Consulter la Résolution du Conseil d'administration du 23 juillet 2019 à : https://features.icann.org/consideration-ssac-advisory-regarding-access-domain-name-registration-data-sac101

questions de politique fondamentales, il faudra suivre ces principes non justifiés figurant à la Recommandation 14.2.

4) Il n'est pas nécessaire d'obliger les requérants à « endosser en premier lieu les frais d'entretien du système ». Le recours à des fonds de l'ICANN constitue une alternative viable.

Le SSAD représente le système d'accès à plusieurs niveaux projeté de longue date que la communauté de l'ICANN a anticipé comme étant une fonctionnalité du système RDS. [147] Les services d'enregistrement des données sont un service essentiel, offert par les parties contractantes en tant que ressource publique. [148] Tel que nous l'anticipons depuis des années, l'accès différentié / à plusieurs niveaux est à présent exigé par l'évolution de la loi. Le SSAD offrira ainsi un service d'intérêt public essentiel. Ce n'est donc pas logique que la Recommandation 14 interdise pratiquement aux frais provenant de l'enregistrement des domaines d'être utilisés pour le fonctionnement du système.

Le recours au financement de l'ICANN s'inscrit pleinement dans le cadre de sa mission. La Spécification temporaire nous rappelle également que l'ICANN s'engage entièrement à « maintenir le système WHOIS existant autant que possible », et que « la mission de l'ICANN implique de faciliter directement à un tiers le traitement des données pour des finalités légitimes et proportionnées, liées à l'application de la loi, la concurrence, la protection des consommateurs, la confiance, la sécurité, la stabilité, la résilience, les usages malveillants, la souveraineté et la protection des droits ». Pour en savoir davantage sur les engagements de l'ICANN en ce sens, consulter la section 5.4. du document SAC101v2.[149]

Autres exemples similaires : le service centralisé de données de zone (CZDS) a été conçu et maintenu par des financements ICANN. L'ICANN procède ainsi car les fichiers de zone constituent une ressource essentielle utilisée pour des finalités légitimes par une grande variété d'utilisateurs. Le CZDS apporte des avantages non seulement à ceux qui l'utilisent mais aussi aux parties contractantes qui peuvent ainsi gérer aisément les inscriptions à ces fichiers de zone. Le SSAD, qui est un cas de figure similaire, a été conçu pour bénéficier tant les requérants que les parties contractantes.

5) Cette phrase est un ajout de dernière minute à la Recommandation 14. « En outre, les personnes concernées ne DOIVENT PAS endosser les frais du traitement des requêtes de divulgation des données qui ont été refusées par les parties contractantes

[147] La communauté de l'ICANN a conçu l'accès différentié ou à plusieurs niveaux comme une fonctionnalité future du service d'annuaire de données d'enregistrement. À titre d'exemple, le protocole RDAP a été spécifiquement conçu pour fournir un accès différentié / à plusieurs niveaux, la communauté comprenant que les lois en matière de vie privée peuvent exiger que certaines données soient partagées avec des utilisateurs autorisés. À présent, le SSAD est considéré comme un moyen de fournir des données sensibles (employant ou non le RDAP).
[148] Consulter le document SAC101v2., section page 4.
[149] https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf

suite à l'évaluation de la requête soumise par les utilisateurs du SSAD ». Les raisons de cet ajout ne sont pas claires et remettent en question le fait que les frais d'évaluation des demandes de données puissent être transférés aux titulaires de noms de domaine de quelque façon que ce soit, même dans les cas de figure les plus courants.

6) La Recommandation indique : « Les personnes concernées NE DOIVENT PAS payer des frais séparés à la passerelle centrale lorsque leurs données sont requises par ou divulguées à des tiers. ». Il ne semble pas logique que la passerelle centrale puisse exiger des frais aux titulaires de noms de domaine. La passerelle centrale n'a aucune relation commerciale avec les titulaires de noms de domaine.

7) Les actions des *titulaires de noms de domaine* sont en général à l'origine de la demande de données des tiers.

8) Le SSAC ignore si la Recommandation 14 violera le RGPD.

La Recommandation 14 (y compris le point 14.6) envisage que les requérants assument les frais de requête de données. Les frais d'utilisation sont la seule façon d'aboutir au modèle de recouvrement des coûts prévu par les Recommandations 14.2 et 14.6, et de ne pas transférer les coûts aux titulaires de noms de domaine / personnes concernées.

En vertu du RGPD, si les personnes concernées souhaitent recevoir, actualiser ou demander la suppression de leurs données, ils n'ont pas à payer de frais pour ce faire.[150] Aux termes du RGPD, les tiers ayant des intérêts légitimes peuvent recevoir des données lorsque leur droit à le faire l'emporte sur l'intérêt des personnes concernées. Dans le cadre du SSAD, les tiers feront ce genre de demande car ils peuvent légitimement invoquer que leurs droits sont en train d'être violés par la personne concernée (titulaire de nom de domaine). L'EPDP n'a pas analysé si les frais pour les requêtes des tiers sont autorisés par le RGPD, et dans quelles circonstances. Même après que le SSAC ait proposé de soumettre cette question à un avis juridique externe, l'EPDP ne l'a pas fait.

Ce problème peut être évité si l'ICANN subventionne le SSAD.

8 Autres commentaires

Veuillez trouver ci-dessous des commentaires sur d'autres recommandations que le SSAC ne rejette pas mais considère néanmoins comme pouvant être améliorées. Nous soumettons ces commentaires à la considération de la GNSO.

[150] Consulter l'article 15 du RGPD, l'article 57(4), et le guide du bureau du commissaire aux informations : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/. Le RGPD autorise le paiement de frais par les personnes concernées uniquement lorsque leurs requêtes s'avèrent « manifestement non-fondée et excessives ». Dans le SSAD, les requêtes de données non-fondées ou excessives, non autorisées, seront rejetées.

Concernant la Recommandation 14 :
La Recommandation 14.8 comporte des lacunes et ne semble pas nécessaire. Il y est dit : « Lors de la mise en œuvre et de l'exploitation du SSAD il faut veiller à ne pas faire peser trop de poids sur les opérateurs les plus petits ». Nous estimons que la formule « ne pas faire peser trop de poids sur les opérateurs les plus petits » n'est ni claire ni transparente. Il est clair que tout bureau d'enregistrement et opérateur de registre, quelle que soit sa taille, devra utiliser le SSAD. Des efforts même minimes pour utiliser le système seront nécessaires de la part des opérateurs. C'est le prix à payer pour faire des affaires au niveau des gTLD et pour maintenir l'accréditation auprès de l'ICANN. Nous craignons que la Recommandation 14.8 ne soit utilisée dans le but de priver le SSAD de certaines fonctionnalités qui lui sont pourtant nécessaires.

La section des orientations relatives à la mise en œuvre de la Recommandation 14 devrait également être révisée en conséquence.

La Recommandation 1.2.3 stipule que : « Les recommandations relatives aux activités du SSAD et aux politiques développées par le Comité permanent doivent obtenir le consensus des membres du comité afin de pouvoir remettre des recommandations formelles au conseil de la GNSO. Pour que les recommandations obtiennent une désignation par consensus, **le soutien des parties contractantes s'avère nécessaire** ». (caractères gras ajoutés)

Le Comité permanent peut faire deux types de commentaires :

- Le premier concerne des recommandations pour des changements contractuels contraignants. Pour qu'elles soient entérinées, la GNSO doit obtenir un vote à la majorité qualifiée en vertu des statuts constitutifs de l'ICANN. Cela implique l'approbation des parties contractantes.
- L'autre type de commentaire concerne des recommandations de mise en œuvre. Celles-ci ne deviennent pas exécutoires pour les parties contractantes.

Le problème est que la Recommandation 18 applique la règle de la majorité qualifiée dans les deux cas alors qu'elle ne devrait s'appliquer que dans le premier. Telle qu'elle est formulée, la Recommandation 18 donne aux parties contractantes un pouvoir de vote sur les choix de mise en œuvre. Or, à notre connaissance, le fait de donner à une partie ou à une chambre un droit de véto sur ce type de décision ne constitue par une procédure décisionnelle habituelle de la GNSO.[151]

[151] Nous ne voyons pas comment les questions de mise en œuvre pourraient entrer dans le cadre du processus d'orientation de la GNSO, qui requiert une majorité qualifiée.

Un problème d'ordre pratique est que nous ignorons si les SO/AC souhaiteront prendre part au Comité permanent dans le cas où les questions de mise en œuvre puissent faire l'objet d'un véto de la part d'un ou de deux participants.

Nous ne voyons pas comment les questions de mise en œuvre pourraient entrer dans le cadre du processus d'orientation de la GNSO, lequel requiert une majorité qualifiée.

9 Remerciements, manifestation d'intérêts, désaccords, visions alternatives et rétractations

Dans un souci de transparence, ces sections fournissent au lecteur des informations relatives à quatre aspects du processus du SSAC. La section « Remerciements » répertorie les membres du SSAC, en dehors des experts et du personnel de l'ICANN, qui ont contribué directement à l'élaboration de ce document en particulier. La section « Manifestations d'intérêt » présente la biographie de tous les membres du SSAC, qui divulguent tous les intérêts susceptibles de soulever un conflit (réel, apparent ou potentiel) avec la participation d'un membre dans la préparation du présent rapport. La section « Désaccords et visions alternatives » permet aux membres individuels de faire état de tout désaccord ou vision alternative concernant le contenu de ce document ou de son processus de préparation. La section « Rétractations » identifie les membres individuels qui se sont récusés des débats concernant le sujet du présent rapport. À l'exception des membres dont le nom apparaît dans les sections « Désaccords et visions alternatives » et « Rétractations », le présent document a été approuvé par consensus de l'ensemble des membres du SSAC.

9.1 Remerciements

Le comité tient à remercier les membres du SSAC ci-dessous ainsi que toutes les personnes ayant contribué à l'élaboration de ce rapport pour leur temps, leurs contributions et leurs révisions.

Membres du SSAC
Greg Aaron
Benedict Addis
Ben Butler
Steve Crocker
James Galvin
John Levine
Rod Rasmussen
Tara Whalen

Personnel de l'ICANN
Andrew McConachie
Danielle Rutherford

Kathy Schnitt
Steve Sheng (rédacteur)

9.2 Manifestations d’''intérêt

Les informations biographiques des membres du SSAC et les manifestations d’intérêt sont disponibles sur : https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

9.3 Désaccords et visions alternatives

Aucun désaccord ni approche alternative.

9.4 Rétractations

Aucune rétractation.

Annexe F - Contributions de la communauté

F.1. Appel à contributions des SO, AC, SG et C :

Selon le manuel PDP de la GNSO, une équipe consacrée à un PDP devrait solliciter formellement des déclarations de chaque groupe de représentants et de chaque unité constitutive de la GNSO dans les premières étapes de ses délibérations. Une équipe responsable de l'EPDP est également invitée à rechercher l'opinion d'autres comités consultatifs et organisations de soutien de l'ICANN ayant l'expertise, l'expérience ou un intérêt particulier dans la problématique examinée. En conséquence, l'équipe a demandé la contribution de toutes les organisations de soutien et de tous les comités consultatifs de l'ICANN ainsi que des unités constitutives et des groupes des représentants de la GNSO au début de ses délibérations sur l'étape 2. En réponse, des déclarations ont été reçues de :

- L'unité constitutive des utilisateurs commerciaux de la GNSO (BC)
- Le groupe des représentants des entités non commerciales (NCSG)
- Le groupe des représentants des opérateurs de registres (RySG)
- Le groupe des représentants des bureaux d'enregistrement (RrSG)
- L'unité constitutive des fournisseurs de services Internet et de services de connectivité (ISPCP)

Les déclarations complètes se trouvent à l'adresse suivante : https://community.icann.org/x/zIWGBg.

Toutes les contributions reçues ont été ajoutées à l'outil d'examen des contributions précoces et prises en compte par l'équipe responsable de l'EPDP.

F.2. Forum de consultation publique sur le rapport initial

Le 7 février 2020, l'équipe responsable de l'EPDP a publié son rapport initial pour consultation publique. Le rapport initial décrivait les questions fondamentales discutées à propos du système normalisé proposé d'accès et de divulgation des données d'enregistrement des gTLD non publiques (« SSAD ») et les recommandations préliminaires qui l'accompagnaient.

L'équipe responsable de l'EPDP a utilisé un formulaire Google pour faciliter l'analyse des commentaires publics. Quarante-cinq contributions ont été reçues des groupes de représentants et des unités constitutives de la GNSO, des comités consultatifs de l'ICANN, d'entreprises et d'organisations, en plus de deux contributions individuelles. Les commentaires sont disponibles à l'adresse suivante: https://docs.google.com/spreadsheets/d/1EBiFCsWfqQnMxEcCaKQywCccEVdBc9_ktPA3PU8nrQk/edit?usp=sharing.

Afin de faciliter son analyse des commentaires publics, l'équipe responsable de l'EPDP a mis au point un ensemble d'outils d'analyse des commentaires publics (PCRT) et des tables de discussion (consulter https://community.icann.org/x/Hi6JBw). À travers l'examen en ligne et les séances plénières, l'équipe responsable de l'EPDP a terminé son analyse et son évaluation des commentaires reçus et convenu des modifications à apporter aux recommandations et/ou au rapport.

F.3. Commentaire public sur le supplément

Le 26 mars 2020, l'équipe responsable de l'EPDP a publié un supplément à son rapport initial pour consultation publique. Ce supplément concerne les recommandations et/ou les conclusions préliminaires de l'équipe responsable de l'EPDP sur les thématiques ci-dessus, incluses dans le groupe de priorité 2.

L'équipe responsable de l'EPDP a utilisé un formulaire Google pour faciliter l'analyse des commentaires publics. Vingt-huit contributions ont été reçues des groupes de représentants et des unités constitutives de la GNSO, des comités consultatifs de l'ICANN, d'entreprises et d'organisations, en plus d'une contribution individuelle. Les commentaires sont disponibles à l'adresse suivante: https://docs.google.com/spreadsheets/d/1jN5ThNtmcVJ8txdAGw0ynl5vrGJOuEv8xeccvzjR9qM/edit#gid=2086811131.

Afin de faciliter son analyse des commentaires publics, l'équipe responsable de l'EPDP a mis au point un ensemble d'outils d'analyse des commentaires publics (PCRT) et des tables de discussion (consulter https://community.icann.org/x/Hi6JBw). À travers l'examen en ligne et les séances plénières, l'équipe responsable de l'EPDP a terminé son analyse et son évaluation des commentaires reçus et convenu des recommandations et/ou des conclusions de priorité 2 qui étaient prêtes pour leur inclusion dans le présent rapport final.

Annexe G – Comité juridique

Questions de l'étape 2 soumises à Bird & Bird

1. Envisagez un système normalisé d'accès/de divulgation dans lequel :

    - aux termes des dispositions contractuelles, les parties contractantes (« CP ») sont tenues par l'ICANN de divulguer les données d'enregistrement, y compris les données à caractère personnel,
    - les données doivent être divulguées aux requérants via RDAP directement ou par l'intermédiaire d'un organisme d'accréditation/autorisation de requête intermédiaire,
    - l'accréditation est effectuée par un tiers commandé par l'ICANN sans implication de la CP
    - la divulgation s'effectue de manière automatisée sans intervention manuelle,
    - les personnes concernées sont dûment informées, conformément aux exigences contractuelles de l'ICANN, des fins auxquelles les données à caractère personnel peuvent être traitées et par quels types d'entités. Le contrat des CP avec l'ICANN exige également que les CP informent la personne concernée de cette divulgation potentielle et de ce traitement par un tiers avant que la personne concernée ne conclue un contrat d'enregistrement avec la CP, et à nouveau annuellement par le biais du rappel d'exactitude des données d'enregistrement exigé par l'ICANN. La partie contractante l'a fait.

    Par ailleurs, supposez que les mesures de protection suivantes sont en place :

    - L'ICANN ou son délégué a validé/vérifié l'identité du requérant et a exigé dans chaque instance que le requérant :
        - démontre qu'il se fonde sur une base légitime pour demander et traiter les données,
        - présente son fondement légitime,
        - indique qu'il ne demande que les données nécessaires à sa finalité,
        - accepte de traiter les données conformément au RGPD, et
        - accepte les clauses contractuelles standard de l'UE pour le transfert de données.

    - L'ICANN ou son délégué consigne les requêtes de données d'enregistrement non publiques, vérifie régulièrement ces journaux, prend des mesures de conformité contre les abus présumés et met ces journaux à disposition sur demande de la personne concernée.

    1. Quel risque ou quelle responsabilité, le cas échéant, la partie contractante pourrait-elle devoir assumer pour la divulgation comme activité de traitement dans

ce contexte, y compris le risque qu'un tiers utilise de mauvaise foi ou contourne les garanties ?

2. Considérez-vous que les critères et les garanties décrits ci-dessus sont suffisants pour rendre la divulgation des données d'enregistrement conforme ? S'il existe un risque, quelles mesures de protection améliorées ou supplémentaires élimineraient[1] ce risque ?

3. Dans ce scénario, la CP serait-elle une autorité de contrôle ou un traiteur[2] et dans quelle mesure, le cas échéant, la responsabilité de la CP serait-elle affectée par cette distinction entre autorité de contrôle et traiteur ?

4. Répondez uniquement s'il existe toujours un risque pour la CP : S'il existe encore un risque pour la CP, quelles garanties supplémentaires pourraient être nécessaires pour éliminer la responsabilité de la CP selon la nature de la demande de divulgation, c'est-à-dire selon que les données sont demandées, par exemple, par des acteurs privés qui intentent des poursuites civiles ou par les autorités chargées de l'application de la loi en fonction de leur juridiction ou de la nature du délit (délit mineur ou crime) ou des sanctions y associées (amende, emprisonnement ou peine capitale) ?

Note 1 : « Il est important ici de souligner le rôle particulier que les garanties peuvent jouer pour réduire l'impact abusif sur les personnes concernées, et donc de modifier l'équilibre des droits et des intérêts dans la mesure où les intérêts légitimes de l'autorité de contrôle de données ne seront pas outrepassés ».
(https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf)

Note 2 : https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

2. Dans quelle mesure, le cas échéant, les parties contractantes sont-elles responsables lorsqu'un tiers accrédité pour la finalité indiquée accède à des données WHOIS non publiques et s'engage à certaines garanties raisonnables similaires à un code de conduite concernant l'utilisation des données, mais fausse les fins prévues pour le traitement de ces données, et les traite par la suite d'une manière incompatible avec la finalité déclarée ? Dans de telles circonstances, s'il existe une possibilité de responsabilité envers les parties contractantes, y a-t-il des mesures qui puissent être prises pour atténuer ou réduire le risque de responsabilité envers les parties contractantes ?

3. En supposant qu'il existe une politique qui permet aux parties accréditées d'accéder à des données WHOIS non publiques par le biais d'un SSAD (et que ladite politique exige que la partie accréditée s'engage à respecter certaines garanties raisonnables

semblables à un code de conduite), est-il légalement permis en vertu de l'article 6(1)f) de :

- définir des catégories spécifiques de requêtes émanant de parties accréditées (par exemple, réponse rapide à une attaque d'un logiciel malveillant ou contacter avec un contrevenant IP non réactif), pour lesquelles il pourrait y avoir des soumissions automatisées pour des données WHOIS non publiques, sans avoir à vérifier manuellement les qualifications des parties accréditées pour chaque requête de divulgation individuelle, et/ou
- permettre la divulgation automatisée de ces données, sans nécessiter un examen manuel par l'autorité de contrôle ou le traiteur de chaque demande de divulgation individuelle.

En outre, s'il n'était pas possible d'automatiser l'une de ces étapes, veuillez fournir des directives sur la façon d'effectuer le test d'équilibrage en vertu de l'article 6(1)(f).

À titre de référence, veuillez vous reporter aux mesures de protection possibles suivantes :

- La divulgation est requise dans le cadre du contrat des CP avec l'ICANN (résultant de la politique de l'étape 2 de l'EPDP).
- Le contrat des CP avec l'ICANN exige que les CP notifient la personne concernée des finalités pour lesquelles, et les types d'entités par lesquelles, les données à caractère personnel peuvent être traitées. La CP est tenue d'informer la personne concernée de cette possibilité de s'exclure avant que la personne concernée ne conclue un contrat d'enregistrement avec la CP, et à nouveau annuellement par le biais du rappel d'exactitude des données d'enregistrement exigé par l'ICANN. La partie contractante l'a fait.
- L'ICANN ou son délégué ont validé l'identité du requérant et ont exigé que le requérant :
  - démontre qu'il se fonde sur une base légitime pour requérir et traiter les données,
  - fournit sa base légitime,
  - indique qu'il ne demande que les données nécessaires à sa finalité,
  - accepte de traiter les données conformément au RGPD, et
  - accepte les clauses contractuelles standard pour le transfert de données.
- L'ICANN ou son délégué consigne les requêtes de données d'enregistrement non publiques, vérifie régulièrement ces journaux, prend des mesures de conformité contre les abus présumés et met ces journaux à disposition sur demande de la personne concernée.

4. En vertu du RGPD, une autorité de contrôle peut divulguer des données à caractère personnel à l'autorité compétente en matière d'application de la loi en vertu de l'article 6(1)(c) du RGPD à condition que l'autorité chargée de l'application de la loi ait l'autorité

juridique de créer une obligation juridique aux termes de la loi applicable. Certains commentateurs ont interprété l'« obligation juridique » comme ne s'appliquant qu'aux obligations juridiques fondées sur le droit de l'UE ou des États membres.

Quant à l'autorité de contrôle de données :

a. Par conséquent, l'autorité de contrôle de données ne peut-elle pas se fier à l'article 6(1)(c) du RGPD pour divulguer des données à caractère personnel aux autorités chargées de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ? Ou bien existe-t-il des circonstances dans lesquelles les autorités de contrôle pourraient s'appuyer sur l'article 6(1)(c) du RGPD pour divulguer des données à caractère personnel aux autorités policières en dehors de la juridiction de l'autorité de contrôle ?

b. L'autorité de contrôle peut-elle se fonder sur d'autres bases juridiques, outre l'article 6(I)(f) du RGPD, pour divulguer des données à caractère personnel aux autorités responsables de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ?

Pour ce qui est de l'autorité chargée de l'application de la loi :

Étant donné que l'article 6 1 du RGPD stipule que les autorités publiques européennes ne peuvent pas utiliser l'article 6(I)(f) du RGPD comme base juridique pour le traitement effectué dans l'accomplissement de leurs tâches, ces autorités publiques doivent avoir une autre base juridique pour que la divulgation puisse avoir lieu (par exemple, l'article 6(I)(c) du RGPD).

c. À la lumière de cela, est-il possible pour les autorités chargées de l'application de la loi non basées dans l'UE de s'appuyer sur l'article 6(I)(f) du RGPD comme base juridique pour leur traitement ? Dans ce contexte, l'autorité de contrôle de données peut-elle se fonder sur l'article 6(1)(f) du RGPD pour divulguer les données à caractère personnel ? Si les autorités chargées de l'application de la loi non basées dans l'UE ne peuvent pas se fonder sur l'article 6(1)(f) du RGPD comme base juridique pour leur traitement, sur quelle base peuvent-elles s'appuyer ?

- Résumé analytique[152]

Questions 1 et 2

Résumé analytique :
L'équipe responsable de l'étape 2 de l'EPDP a envoyé sa première série de questions à Bird & Bird le 29 août 2019. Bird & Bird a répondu à ce lot de questions dans une série de trois notes. La note 1 a été livrée le 9 septembre 2019. La note 1 a analysé le rôle juridique des parties

[152] À mettre à jour lorsque le Comité juridique aura approuvé les résumés analytiques

contractantes dans le système normalisé proposé d'accès et de divulgation (SSAD), la suffisance des garanties proposées et le risque de responsabilité des parties contractantes pour la divulgation à travers le SSAD. Les questions envoyées à Bird & Bird sont fournies dans l'annexe du présent document et incluent une série d'hypothèses aux sections 1.1 et 1.2 qui font partie des fondements factuels des réponses ci-dessous.

En réponse à ces questions, Bird & Bird a noté ce qui suit en ce qui concerne le contrôle :

1. Les parties contractantes sont des autorités de contrôle probables dans le SSAD puisque les titulaires de noms de domaine s'attendent traditionnellement et raisonnablement à ce que les parties contractantes contrôlent la divulgation de leurs données à des tiers. Il est difficile de montrer que les parties contractantes ne servent que les intérêts de l'organisation ICANN, en particulier à la lumière des décisions judiciaires pertinentes qui suggèrent un seuil bas pour le contrôle.
2. Si l'équipe responsable de l'EPDP voulait recommander une politique en vertu de laquelle les parties contractantes seraient des responsables du traitement dans un SSAD, des mesures pourraient être prises pour soutenir cet objectif de politique. Les parties contractantes n'auraient pas besoin d'avoir d'influence importante sur les aspects clés du traitement des données du SSAD, tels que (i) les données qui seront traitées ; (ii) la durée de leur traitement ; et (iii) les personnes qui auront accès aux données. Il faudrait également une supervision « constante et prudente » par l'organisation ICANN « pour assurer la conformité complète du traiteur avec les instructions et les termes du contrat », et des efforts pour informer les titulaires de noms de domaine que les parties contractantes agissent uniquement au nom de l'organisation ICANN (par exemple, les documents du site Web de l'organisation ICANN, les avis de confidentialité, les informations dans le processus d'enregistrement des noms de domaine).
3. Cependant, le résultat le plus probable et la position de départ pour les autorités de surveillance serait que les parties contractantes soient des responsables du traitement et probablement des responsables conjoints du traitement avec l'organisation ICANN concernant la divulgation des données d'enregistrement par le biais du SSAD.

Bird & Bird a noté ce qui suit en ce qui concerne les garanties et la responsabilité du SSAD :

4. Compte tenu du nombre de juridictions impliquées et de la variété probable de requêtes pouvant être traitées par le SSAD, Bird & Bird ne pourrait pas confirmer que les critères et les garanties décrits dans les hypothèses feraient que la divulgation de données dans un SSAD entièrement automatisé soit conforme.
5. Bird & Bird a suggéré des garanties supplémentaires que l'EPDP devrait prendre en considération en ce qui concerne (i) la base juridique, la proportionnalité et la

minimisation des données ; (ii) les droits individuels ; (iii) le transfert international des données ; et (iv) la sécurité.

6. En vertu du RGPD, les parties impliquées dans le même traitement sont responsables envers les individus et les autorités de surveillance. La responsabilité individuelle est conjointe et solidaire, ce qui signifie que chaque partie impliquée dans le traitement est potentiellement responsable de tous les dommages à la personne concernée, des normes différentes s'appliquant aux autorités de contrôle et aux traiteurs. Les autorités de surveillance pourraient procéder contre les autorités de contrôle ou les traiteurs, et il est actuellement difficile de savoir si la responsabilité conjointe et solidaire s'applique lorsque plusieurs parties sont impliquées dans le même traitement (c'est-à-dire que les mesures d'application ne sont pas appropriées si d'autres sont responsables).

---

1. Les parties contractantes sont-elles des autorités de contrôle ou des traiteurs ?

Autorités de contrôle

- La responsabilité change considérablement si les parties contractantes sont des autorités de contrôle ou des traiteurs. (1.4)
- Une autorité de contrôle est la « personne physique ou morale, l'autorité publique, l'organisme ou toute autre entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel ». (2.2)
- Le caractère d'autorité de contrôle d'une entité correspond à une détermination factuelle fondée sur le « contrôle des décisions au sujet du traitement de données clés ». Le rôle d'autorité de contrôle ne peut pas être attribué ou refusé. (2.3)
- Le Groupe de travail Article 29 a fourni des directives préalables au RGPD sur les rôles de l'autorité de contrôle et du traiteur. Le CEPD est en train de réviser ces directives et prévoit de la mettre à jour au cours des six prochains mois. (2.4 et 2.19)
- Le prédécesseur du CEPD, le Groupe de travail Article 29 sur la protection de données (WP29), a déterminé que « le rôle premier de l'autorité de contrôle est de déterminer qui sera responsable du respect des règles de protection des données et comment les personnes concernées peuvent exercer les droits dans la pratique. Autrement dit : de répartir les responsabilités ». Lu littéralement, cela reflète qu'une autorité de contrôle a la responsabilité de la plupart des obligations en vertu du RGPD ; mais l'expression indique également un degré d'efficacité réglementaire : il montre la nécessité sous-jacente d'avoir un responsable. De l'avis de B&B, cela peut influencer l'approche d'un tribunal ou d'une autorité de surveillance. (2.4)

- Une entité qui prend des décisions clés (seule ou conjointement avec d'autres) concernant (i) les données traitées ; (ii) la durée du traitement ; et (iii) qui a accès aux données agit comme une autorité de contrôle, et non comme un traiteur – ces données sont parfois appelées les « éléments essentiels » du traitement. (2.6)

- Une entité peut être à la fois une autorité de contrôle et un traiteur. Ce sera le cas lorsqu'une entité qui agit en tant que traiteur utilise également des données à caractère personnel à ses propres fins. (2.7)

Traiteurs

- Traiteur de données tel qu'utilisé dans le présent document désigne « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui traite des données à caractère personnel pour le compte de l'autorité de contrôle ». (2.5)

- Les directives du Groupe de travail Article 29 soulignent l'importance d'examiner « le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables des personnes concernées sur la base de cette visibilité » pour déterminer si une entité est une autorité de contrôle ou un traiteur. (2.5)
- Selon le WP29, un traiteur sert « l'intérêt de quelqu'un d'autre » en « mettant en œuvre les instructions données par l'autorité de contrôle au moins en ce qui concerne l'objectif du traitement et les éléments essentiels des moyens ». (2.5)

- Un traiteur ne peut traiter les données à caractère personnel que conformément aux instructions de l'autorité de contrôle ou conformément à la législation de l'EEE ou des États membres. (2.7)

Candidature au SSAD

Présomption de contrôle

- Dans certains cas, « les rôles traditionnels existants qui impliquent normalement une certaine responsabilité aideront à identifier l'autorité de contrôle : par exemple, l'employeur en ce qui concerne les données sur ses employés, l'éditeur en ce qui concerne les données sur les abonnés, l'association en ce qui concerne les données sur ses membres ou contributeurs ». La relation entre une partie contractante et un titulaire de nom de domaine (ou le contact du titulaire de nom de domaine) pourrait être considérée de la même manière. (2.8) De même, « l'image donnée aux personnes concernées et les attentes raisonnables des personnes concernées » sont un facteur important pour déterminer l'autorité de contrôle. Un titulaire de nom de domaine s'attend généralement à ce que les parties contractantes soient l'autorité de contrôle de la divulgation de leurs données à des tiers. (2.9)

- Étant donné que les parties contractantes sont actuellement considérées comme l'autorité de contrôle de la divulgation des données à des tiers, cela entraînera une présomption que les parties contractantes continuent de l'être, même une fois qu'un SSAD sera mis en œuvre. (2.9)

- Toutefois, on ne peut pas toujours avoir une telle présomption ; cela dépendra de l'analyse des activités de traitement technique. Le WP169 note que lorsqu'il existe une hypothèse selon laquelle une personne est une autorité de contrôle (appelé dans le WP169 « contrôle découlant de la compétence implicite »), cela ne devrait être le cas que « sauf si d'autres éléments indiquent le contraire ». Des cas récents de la CJUE – en particulier sa récente décision Fashion ID – ont également soutenu une analyse plus étroite et factuelle. (2.11)

Difficulté à présenter les parties contractantes comme agissant « au nom de » quelqu'un d'autre

- L'élément le plus important du rôle d'un traiteur est qu'il n'agit que pour le compte de l'autorité de contrôle. Il sera difficile de montrer que les parties contractantes ne servent que les intérêts de l'ICANN et ne traitent les données que pour le compte de l'ICANN. (2.10)

- La divulgation de données est susceptible d'être considérée comme une conséquence inévitable du fait d'être une partie contractante, et non pas quelque chose que les parties contractantes acceptent de faire au nom de l'ICANN. (2.10)

Analyse factuelle détaillée des activités de traitement technique

- Le seuil factuel pour devenir une autorité de contrôle (détermination des finalités ou des moyens de traitement) est faible. Selon la CJUE, le test vise simplement à savoir si quelqu'un « exerce une influence sur le traitement des données à caractère personnel, à ses propres fins, et (…) participe, par conséquent, à la détermination des finalités et des moyens de ce traitement ». (2.12)

- Dans la décision de Jehovan Todistajat de la CJUE, l'organisation nationale de la communauté des témoins de Jéhovah a été déclarée comme ayant des « connaissances générales » et ayant encouragé et coordonné la collecte de données par les membres de la communauté (prédicateurs de porte à porte) à un niveau très général – mais il a néanmoins été jugé satisfait du test de contrôle conjoint avec ces membres de la communauté. Dans la décision de la CJUE sur Fashion ID, il suffisait à l'opérateur du site Web de s'intégrer au code de la plateforme Facebook, de sorte que l'opérateur a participé à la détermination des « moyens » de collecte de données de Facebook et qu'il était un responsable conjoint du traitement avec Facebook. (2.14)

- Les tribunaux et les autorités de surveillance sont donc susceptibles de considérer qu'une partie contractante est impliquée dans la détermination des moyens de

traitement, peut-être simplement en raison de la mise en œuvre/l'interaction avec le SSAD. (2.14)

Facteurs potentiellement à l'appui du statut de traiteur

- La clé pour éviter le statut d'autorité de contrôle est de pouvoir montrer que l'on n'est pas impliqué dans la détermination des « éléments essentiels » du traitement (2.6).
- En outre, la surveillance par l'ICANN de la conformité avec l'exigence contractuelle de divulguer des données pourrait être la preuve d'une action de l'autorité de contrôle en tant que traiteur, puisque « une surveillance constante et minutieuse par l'autorité de contrôle pour assurer la conformité complète du traiteur avec les instructions et les termes du contrat fournit un indice que l'autorité de contrôle est toujours en pleine et entière maîtrise des opérations de traitement ». (2.16)
- La prise de mesures pour informer clairement les personnes concernées que les données sont collectées uniquement pour le compte de l'ICANN (par exemple, les divulgations dans le processus d'enregistrement de noms de domaine, le rappel annuel sur l'exactitude des données, les avis de confidentialité, les documents publiés sur le site Web de l'organisation ICANN) et la diffusion d'autres présentations qui décrivent clairement cette action comme étant effectuée par les parties contractantes uniquement pour le compte de l'ICANN pourraient générer une prise de conscience des personnes à propos du rôle de l'ICANN en tant qu'autorité de contrôle et du rôle des parties contractées en tant que traiteurs. (2.17)

Récapitulatif – Il est fort probable que les parties contractantes soient des responsables conjoints avec l'ICANN en matière de traitement de données

- Le résultat le plus probable et le point de départ pour les autorités de surveillance est que les parties contractantes soient des autorités de contrôle. (2.18)
- Le rôle de l'ICANN dans la détermination de la finalité et des moyens de traitement suggère qu'ils sont des responsables conjoints du traitement avec les parties contractantes pour la divulgation de données à des tiers. (2.18)

2. Les garanties proposées sont-elles suffisantes pour mettre en conformité la divulgation des données d'enregistrement ?

Garanties du SSAD

- Compte tenu du nombre de juridictions impliquées et de la variété probable de requêtes pouvant être traitées par le SSAD, le présent avis ne pourrait pas confirmer que les critères et les garanties décrits dans les hypothèses feraient que la divulgation de données dans un système entièrement automatisé soit conforme. (3.8)
- B&B déclare que le traitement des données à caractère personnel doit faire l'objet de précautions -- un traiteur (soit en violation de son contrat avec l'autorité de contrôle,

soit autrement se comportant de manière incompatible avec les instructions de l'autorité de contrôle) peut devenir lui-même une autorité de contrôle, et donc faire face aux conséquences des violations (comme indiqué dans le tableau à la page 7 de la note). (3.6)

- Les garanties décrites sont utiles, mais devront inclure les mesures supplémentaires ci-dessous. (3.8)
    - Base juridique : Les garanties doivent (i) déterminer si les parties contractantes, et pas seulement le requérant, se fondent sur une base juridique pour le traitement ; (ii) tenir compte du cadre juridique particulier applicable à la partie contractante ; (iii) assurer qu'un test d'équilibrage approprié soit effectué sur les intérêts légitimes, si c'est une base juridique appropriée dans un cas donné[153] (et qu'il peut ne pas être sûr de supposer que pour une catégorie de requêtes, l'équilibre des intérêts est toujours en faveur de la divulgation ; certains cas, tels que les enquêtes ou les poursuites pouvant entraîner la peine capitale, peuvent être particulièrement problématiques) ; et (iv) assurer que des types ou des volumes de données inappropriés ne seront pas divulgués aux requérants (par exemple, la surveillance basée sur des règles ou le blocage des requêtes de tailles inhabituelles, les systèmes de déclassement). (3.9 à 3.12)
    - Droits individuels : aborder la manière dont les requêtes des personnes concernées sont traitées, y compris (i) les droits d'accès aux journaux des requêtes (qui peuvent eux-mêmes représenter un risque élevé ou même des données à caractère personnel de « catégorie spéciale ») ; (ii) la période de conservation appropriée de ces journaux ; (iii) la manière dont les informations sont fournies aux personnes concernées ; (iv) comment traiter les situations où le requérant insiste pour ne pas fournir d'informations à la personne concernée (p. ex., confidentialité des organismes d'application de la loi) ; et (v) les requêtes de restriction ou de blocage du traitement. (3.13 à 3.16)
    - Transfert de données : pour les transferts internationaux de données, l'EPDP envisage de s'appuyer sur le mécanisme de protection juridique des clauses contractuelles types (SCC) de l'UE. Toutefois, (i) certains requérants, y compris les autorités publiques, n'accepteront pas leurs conditions ; (ii) les conditions des SCC ne sont pas faciles à respecter, en particulier à grande échelle ; (iii) si les parties contractantes de l'EEE sont des traiteurs, elles ne peuvent pas se fier directement aux SCC pour transférer des données à l'organisation ICANN ou aux requérants en dehors de l'EEE et il faudrait donc trouver une solution de contournement. (3.17)

[153] Si la divulgation est une obligation légale en vertu de la législation de l'UE ou des États membres de l'UE/EEE (y compris les traités auxquels l'UE ou un État membre concerné fait partie), il n'est pas nécessaire de considérer le critère des intérêts légitimes.

- Sécurité : les garanties devraient être proportionnelles au risque pour les personnes concernées au cas où leurs données étaient compromises. (3.18)

3. Quel est le risque de responsabilité des parties contractantes pour divulgation ?

- Si les garanties sont inadéquates ou abusées/contournées par les requérants (ou si d'autres aspects du RGPD sont contrevenus, par exemple un avis inadéquat ou l'absence d'une base légale pour le traitement), les parties contractantes pourraient faire l'objet d'enquêtes, d'ordres d'exécution (par exemple, des interdictions de traitement), et (financièrement) la responsabilité à l'égard des individus (civile) et la responsabilité à l'égard des autorités de surveillance (amendes).

- En gros, B&B propose dans les parties pertinentes que (1) lorsque les parties sont des responsables conjoints du traitement, cela ne signifie pas que les parties doivent chacune assumer tous les éléments de la conformité, (2) si les parties contractantes sont des traiteurs, elles ne seront responsables que auprès des personnes (responsabilité civile) en vertu de l'art. 82 si elles n'ont pas respecté les obligations imposées aux traiteurs en vertu du règlement, ou si elles ont agi en dehors ou en contradiction avec les instructions légales de l'autorité de contrôle, (3) même lorsque les parties sont considérées des responsables conjoints du traitement, des décisions judiciaires récentes (concernant l'application par les autorités de surveillance) ont souligné que la responsabilité conjointe du traitement n'implique pas une responsabilité égale pour les violations du RGPD, et (4) les parties contractantes, en tant que responsables conjoints du traitement avec l'organisation ICANN, bénéficieraient d'une répartition claire des responsabilités selon les termes de l'« arrangement » de responsabilité conjointe du traitement qu'elles doivent conclure conformément au Chapitre 26 du RGPD.

Responsabilité envers les individus

- L'article 82 du RGPD énonce les règles relatives à la responsabilité auprès des individus. (4.2)

- Les autorités de contrôle sont responsables des dommages provoqués par un traitement qui viole le RGPD. Les traiteurs sont responsables des dommages provoqués par le traitement lorsque le traiteur n'a pas satisfait aux exigences qui lui sont spécifiques ou lorsqu'il a agi en dehors de ou en contradiction avec les instructions de l'autorité de contrôle. (4.2)

- Une autorité de contrôle ou un traiteur n'est pas responsable si elle démontre qu'elle n'était point responsable de l'événement ayant entraîné les dommages. (4.2)

- Lorsque plusieurs autorités de contrôle ou traiteurs sont impliqués dans le même traitement, chaque entité est responsable de l'ensemble des dommages (responsabilité conjointe et solidaire) auprès des individus (4.2 et 4.3)

- Si les parties contractantes sont des traiteurs, elles ne sont responsables que si elles ne respectent pas les obligations spécifiques aux traiteurs en vertu du RGPD ou si elles agissent en dehors ou en violation des instructions de l'autorité de contrôle. Dans un tel scénario, il est peu probable que les parties contractantes enfreignent les instructions de l'autorité de contrôle parce que le SSAD est automatisé ; la source la plus probable de responsabilité pour elles, par conséquent, serait d'avoir des mesures de sécurité inadéquates, ou de ne pas se conformer aux règles du RGPD sur les transferts internationaux de données. Les parties contractantes pourraient se tourner vers l'organisation ICANN pour prescrire des accords de sécurité et des transferts internationaux afin de donner aux parties contractantes la capacité de faire valoir qu'elles « ne sont point responsables de l'événement ayant entraîné les dommages ». (4.4)

- Si les parties contractantes sont des autorités de contrôle, et si la divulgation viole le RGPD, il est peu probable qu'elles évitent la responsabilité auprès des individus si elles ne peuvent pas démontrer qu'elles « ne sont point responsables de l'événement donnant lieu aux dommages » ou si elles participent activement à l'événement de divulgation.

- Toute responsabilité crée le potentiel que les parties contractantes seraient responsables de tous les dommages à la personne concernée. Ce risque est maximisé dans le cas des responsables conjoints du traitement. (4.5 et 4.6)

- Les parties contractantes tenues responsables de l'intégralité des dommages subis par une personne concernée peuvent demander des contributions appropriées à d'autres parties responsables. (4.7)

- En tant qu'autorités de contrôle, les parties contractantes et l'ICANN auraient l'obligation positive d'affronter le risque que les requérants recherchent un accès inapproprié aux données à caractère personnel. Les garanties doivent être adaptées au niveau du risque. Si un requérant contourne les garanties du SSAD, les tribunaux peuvent accepter que les garanties soient adéquates, ce qui limiterait la responsabilité principale des parties contractantes. (4.9 et 4.10)

- Même en cas d'une violation du RGPD provoquée par un requérant, les parties contractantes, l'ICANN et le requérant peuvent être considérés comme « impliqués dans le même traitement », chaque partie étant conjointement et solidairement responsable des dommages découlant de cette violation. Les parties contractantes et l'ICANN peuvent être en mesure de faire valoir qu'elles « ne sont point responsables de l'événement donnant lieu aux dommages », mais elles devraient autrement demander une compensation au requérant ou inclure le requérant dans la procédure initiale afin de répartir les dommages. (4.11)

  Responsabilité envers les autorités de surveillance

- Les autorités de surveillance peuvent procéder contre les autorités de contrôle ou les traiteurs. (4.12)

- Il n'est pas clair si la responsabilité conjointe et solidaire s'applique lorsque plusieurs parties sont impliquées dans le traitement (c'est-à-dire, une action d'application de la loi n'est sans doute pas appropriée si d'autres sont responsables). (4.13)

- Il faut que la disposition légale soit clairement formulée pour faire valoir la responsabilité conjointe et solidaire. Cela renforce l'argument que cela aurait été expressément déclaré si l'intention des autorités de surveillance était d'imposer des amendes. L'article 83(2)d) indique clairement que la responsabilité conjointe et solidaire ne s'applique pas aux autorités de surveillance. (4.13.2)
- Même lorsque les parties sont des responsables conjoints du traitement, des décisions judiciaires récentes (concernant l'application par les autorités de surveillance) soulignent que le contrôle conjoint n'implique pas une responsabilité égale pour les violations du RGPD. (4.13.4).

- Les parties contractantes et l'ICANN bénéficieraient donc de responsabilités clairement attribuées dans le cadre d'un accord de responsabilité conjointe du traitement (et tel accord est en tout cas obligatoire, dans toutes les situations de responsabilité conjointe du traitement, conformément au Chapitre 26 du RGPD). (4.14)

- Il peut être possible de tirer parti des dispositions du RGPD sur l'« autorité responsable » (alias « guichet unique » ou « cohérence ») pour garantir que toute action d'application soit faite par l'intermédiaire de l'établissement de l'organisation ICANN à Bruxelles, plutôt que contre les parties contractantes. Ce mécanisme n'est disponible que lorsqu'il existe un traitement transfrontalier des données à caractère personnel (entités dans plusieurs États membres de l'EEE, ou effets sur les personnes concernées dans plusieurs États membres de l'EEE). (4.15 à 4.17)

- Les dispositions du RGPD relatives à l'« autorité principale » ne traitent pas spécifiquement des responsabilités conjointes du traitement, mais les directives suggèrent que si l'organisation ICANN et les parties contractantes ont désigné l'établissement belge de l'ICANN comme principal établissement pour le traitement (c'est-à-dire, l'endroit où sont prises les décisions concernant le traitement), cela pourrait minimiser le risque de l'application directement contre les parties contractantes. Il s'agit d'une approche nouvelle et non testée. (4.15 à 4.20)

Annexe :
Questions juridiques 1 et 2 : Responsabilité, garanties, autorité de contrôle et traiteur

Alors que l'équipe responsable de l'EPDP délibère sur l'architecture d'un SSAD, plusieurs questions se sont posées au sujet de la responsabilité et des garanties. En réponse, le Comité

juridique de l'étape 2 a formulé les questions suivantes à l'intention d'un conseiller juridique externe :

1. Envisagez un système normalisé d'accès/de divulgation en vertu duquel :

   o les parties contractantes (« CP ») sont contractuellement tenues par l'ICANN de divulguer les données d'enregistrement, y compris les données à caractère personnel,

   o les données doivent être divulguées aux requérants via RDAP directement ou par l'intermédiaire d'un organisme d'accréditation/autorisation de requête intermédiaire,

   o l'accréditation est effectuée par un tiers commandé par l'ICANN sans implication de la CP,

   o la divulgation s'effectue de manière automatisée sans intervention manuelle,

   o les personnes concernées sont dûment informées, conformément aux exigences contractuelles de l'ICANN, des fins auxquelles les données à caractère personnel peuvent être traitées et par quels types d'entités. Le contrat des CP avec l'ICANN exige également que les CP informent la personne concernée de cette divulgation potentielle et de ce traitement par un tiers avant que la personne concernée ne conclue un contrat d'enregistrement avec la CP, et à nouveau annuellement par le biais du rappel d'exactitude des données d'enregistrement exigé par l'ICANN. La partie contractante l'a fait.

Par ailleurs, supposez que les mesures de protection suivantes sont en place :

- L'ICANN ou son délégué a validé/vérifié l'identité du requérant et a exigé dans chaque instance que le requérant :
  - démontre qu'il se fonde sur une base légitime pour demander et traiter les données,
  - présente son fondement légitime,
  - indique qu'il ne demande que les données nécessaires à sa finalité,
  - accepte de traiter les données conformément au RGPD, et
  - Accepte les clauses contractuelles standard de l'UE pour le transfert de données.
- L'ICANN ou son délégué consigne les requêtes de données d'enregistrement non publiques, vérifie régulièrement ces journaux, prend des mesures de conformité contre les abus présumés et met ces journaux à disposition sur demande de la personne concernée.

a. Quel risque ou quelle responsabilité, le cas échéant, la CP pourrait-elle devoir assumer pour la divulgation comme activité de traitement dans ce contexte, y compris le risque qu'un tiers utilise de mauvaise foi ou contourne les garanties ?

b. Considérez-vous que les critères et les garanties décrits ci-dessus sont suffisants pour rendre la divulgation des données d'enregistrement conforme ? S'il existe un risque, quelles mesures de protection améliorées ou supplémentaires élimineraient154[1] ce risque ?

c. Dans ce scénario, la CP serait-elle un contrôleur ou un traiteur1552 et dans quelle mesure, le cas échéant, la responsabilité du CP serait-elle affectée par cette distinction entre contrôleur et traiteur ?

d. Répondez uniquement s'il existe toujours un risque pour la CP : S'il existe encore un risque pour la CP, quelles garanties supplémentaires pourraient être nécessaires pour éliminer la responsabilité de la CP selon la nature de la demande de divulgation, c'est-à-dire selon que les données sont demandées, par exemple, par des acteurs privés qui intentent des poursuites civiles ou par les autorités chargées de l'application de la loi en fonction de leur juridiction ou de la nature du délit (délit mineur ou crime) ou des sanctions y associées (amende, emprisonnement ou peine capitale) ?

2. Dans quelle mesure, le cas échéant, les parties contractantes sont-elles responsables lorsqu'un tiers accrédité pour la finalité indiquée accède à des données WHOIS non publiques et s'engage à certaines garanties raisonnables similaires à un code de conduite concernant l'utilisation des données, mais fausse les fins prévues pour le traitement de ces données, et les traite par la suite d'une manière incompatible avec la finalité déclarée ? Dans de telles circonstances, s'il existe une possibilité de responsabilité envers les parties contractantes, y a-t-il des mesures qui puissent être prises pour atténuer ou réduire le risque de responsabilité envers les parties contractantes ?

[154]« Il est important ici de souligner le rôle particulier que les garanties peuvent jouer pour réduire l'impact abusif sur les personnes concernées, et donc de modifier l'équilibre des droits et des intérêts dans la mesure où les intérêts légitimes de l'autorité de contrôle de données ne seront pas outrepassés ». https://iapp.org/media/pdf/resource_center/wp217_legitimate-interests_04-2014.pdf

[155]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

Question 3

Résumé analytique :

L'équipe responsable de l'étape 2 de l'EPDP a envoyé sa première série de questions à Bird & Bird le 29 août 2019. Bird & Bird a répondu à ce lot de questions dans une série de trois notes. La note 2 a été remise le 10 septembre 2019 et a analysé les questions relatives à la façon dont le « test d'équilibrage » des intérêts légitimes exigé par l'article 6(1)(f) du RGPD pourrait être appliqué dans un SSAD, soit de manière très automatisée (question A), soit, s'il n'est pas possible d'automatiser une telle décision, comment le test d'équilibrage devrait se faire (question B). Les questions complètes sont fournies dans l'annexe A du présent récapitulatif et incluent une série d'hypothèses qui font partie des fondements factuels des réponses ci-dessous.

En réponse à la question A, Bird & Bird a noté ce qui suit en ce qui concerne l'automatisation :

1. Le processus très automatisé décrit par l'équipe responsable de l'EPDP pourrait se limiter à une prise de décision automatisée ayant un effet juridique ou tout aussi important sur les personnes concernées (« personnes concernées » ici seraient les cibles des requêtes de données gTLD non publiques).
2. Cela n'est généralement pas permis, sauf si l'une des bases juridiques ou exemptions limitées prévues à l'article 22(1) du RGPD justifiait la divulgation. La divulgation serait bien plus limitée que ce que prévoit l'article 6(1)(f) du RGPD. Il serait difficile pour le SSAD, comme proposé, de satisfaire aux exemptions de l'article 22(1) du RGPD. Le SSAD doit donc être structuré de façon à ne pas entrer dans le champ d'application de l'article 22.
3. Pour y parvenir, il serait nécessaire de limiter l'accès/la divulgation automatique aux situations où il n'y aurait pas « d'effets juridiques ou tout aussi importants » pour la personne concernée. Parmi les exemples fournis dans la note, citons la publication des coordonnées de l'administrateur représentant les titulaires qui sont des personnes morales en réponse à des attaques de logiciels malveillants ou à une violation de la propriété intellectuelle. Le processus de traitement des requêtes à risque ne devrait pas être entièrement automatisé ; il devrait y avoir un degré significatif de participation humaine (du moins, à titre de supervision).
4. Alternativement, le SSAD pourrait être structuré de sorte qu'il ne prenne pas de décision fondée sur son traitement automatique des données à caractère personnel relatives aux cibles d'une demande. Par exemple, le SSAD pourrait publier les catégories de requêtes qui seront acceptées et demander aux requérants de confirmer qu'ils répondent aux critères pertinents. Si, plutôt, il était demandé au requérant d'effectuer l'analyse nécessaire et d'informer ensuite le SSAD du résultat, le SSAD ne prendrait alors sans doute pas de décision (de divulguer des données) fondé sur son propre traitement automatisé des données à caractère personnel, de sorte que l'article 22 du RGPD ne

s'appliquerait pas. Toutefois, le fait de dépendre de l'auto-certification par les requérants pourrait générer une possibilité d'abus du système par les requérants, ce qui (comme l'expliquent les réponses précédentes) pourrait signifier une responsabilité pour l'ICANN et les parties contractantes.

5. En ce qui concerne l'authentification du requérant (comme une étape distincte de l'évaluation des motifs ou d'autres paramètres d'une requête), Bird & Bird considère qu'il serait certainement possible d'automatiser le processus d'authentification de la personne qui envoie la requête. Il peut également être possible d'automatiser d'autres aspects du processus de requête.

En réponse à la question B, Bird & Bird :

1. Définit les directives officielles de l'UE (WP29) sur la façon dont le test d'équilibrage des intérêts légitimes de l'article 6(1)f) devrait être mené ;
2. A noté que si l'ICANN et les parties contractantes sont des responsables conjoints du traitement, elles doivent toutes deux établir un intérêt légitime dans le traitement. En ce qui concerne les parties contractantes, il est probable que l'intérêt pertinent soit celui du tiers, le requérant. L'ICANN, en revanche, peut être en mesure d'établir son intérêt à la sécurité, la stabilité et la résilience du système des noms de domaine *ainsi* que l'intérêt du requérant tiers ; et
3. A fourni une discussion de haut niveau sur les garanties qui pourraient être déployées afin de faire pencher davantage les balances en faveur du traitement envisagé dans le cadre du SSAD.

1. Question A

La question A demande si l'article 6(1)(f) du RGPD (la base juridique des « intérêts légitimes » pour le traitement) permettrait au SSAD de traiter automatiquement les requêtes (au moins dans certaines catégories prédéfinies), sans exiger une vérification manuelle, requête par requête (i) que la demande réponde aux critères pertinents de divulgation ; et (ii) la divulgation des données d'enregistrement pertinentes.

Le SSAD pourrait entrer dans le champ d'application de l'article 22 du RGPD, plutôt que d'être lié uniquement à l'article 6(1)(f) du RGPD.

- L'article 6(1)(f) du RGPD permet le traitement automatisé*, sauf* si cela revient à « la prise de décisions individuelles automatisées » ayant des effets juridiques ou tout aussi importants pour la personne concernée (« la prise de décisions exclusivement automatisée »), ce qui n'est généralement pas autorisé, à moins que l'une des bases/exemptions juridiques les plus limitées prévues à l'article 22(1) du RGPD ne justifie la divulgation.

- Bien que l'article 22 du RGPD stipule qu'une personne concernée a le « droit de ne pas être soumis à » une telle décision, dans la pratique, l'article 22 a été interprété par les organismes de règlementation comme une *interdiction* générale (c'est-à-dire qu'il n'est pas nécessaire que la personne concernée s'oppose à une telle prise de décision).

- Le processus décrit par l'équipe responsable de l'EPDP pourrait se traduire par une telle prise de décision automatisée affectant la cible d'une requête (par exemple, lorsque les organismes d'application de la loi souhaitent intenter des poursuites contre des personnes qui exécutent des sites Web illégaux).

- Si l'article 22 s'applique au traitement décrit par l'EPDP, c'est-à-dire **si le traitement du SSAD équivaut à une décision individuelle automatisée ayant des effets juridiques ou tout aussi importants, il ne serait pas permis en vertu de l'article 6(1)(f) du RGPD (la base du traitement des « intérêts légitimes »).** L'article 22(1) définit son propre ensemble de motifs, plus limités, sur lesquels la prise de décisions tel que définie à l'article 22 peut être fondée.

- B&B indique qu'**il sera difficile pour le SSAD de respecter les exemptions prévues à l'article 22(1) ; par conséquent, l'EPDP devrait assurer que le traitement du SSAD ne relève pas du champ d'application de l'article 22.**

Stratégie d'atténuation 1 : éviter les décisions qui pourraient avoir des « effets juridiques ou tout aussi significatifs » pour les personnes dont les données sont divulguées

- Une manière d'y parvenir serait de limiter l'accès et la divulgation automatiques aux situations où il n'y aurait pas « d'effets juridiques ou tout aussi significatifs » pour la personne concernée.

- La décision de divulguer des données par l'intermédiaire du SSAD n'aurait pas en soi un « effet juridique » sur la personne concernée. Le test le plus pertinent pour le SSAD est au niveau des « effets tout aussi significatifs ». Cela signifie quelque chose de semblable à avoir un effet juridique -- quelque chose digne d'attention (par exemple, qui affectent de manière significative les circonstances, le comportement ou les choix des personnes concernées).[156]

- Il peut être possible de déterminer des catégories de requêtes qui n'ont pas d'effet « juridique ou tout aussi significatif » sur la personne, comme la publication des coordonnées administratives pour les titulaires de nom de domaine qui sont des personnes morales (entreprise/organisation/institution). D'autres divulgations impliquant les données d'enregistrement d'une personne physique pourraient avoir un

[156] Selon les directives officielles, voici quelques exemples classiques de décisions qui pourraient être suffisamment importantes : (i) les décisions qui ont un impact sur la situation financière d'une personne ; (ii) les décisions qui touchent l'accès aux services de santé ; (iii) les décisions qui nient les possibilités d'emploi ou qui désavantagent gravement une personne ; (iv) les décisions qui affectent l'accès à l'éducation d'une personne.

« effet tout aussi significatif ». Une grande attention devrait être consacrée à de telles analyses.

- Pour les décisions plus susceptibles d'avoir un « effet significatif », un examen ou une surveillance humaine serait nécessaire. Une participation humaine « symbolique » ne suffirait pas. Pour que l'élément d'évaluation humaine soit pris en compte, l'autorité de contrôle doit assurer une surveillance significative par une personne qui a l'autorité et la compétence nécessaires pour modifier la décision.

Stratégie d'atténuation 2 : Éviter les conceptions d'un SSAD qui impliquent le traitement de données à caractère personnel sur la personne qui fait l'objet une requête afin de décider d'y accéder ou pas.

- Il peut également être possible de structurer le SSAD de sorte qu'il n'implique pas « une décision fondée uniquement sur un traitement automatisé ». L'article 22 du RGPD exige que la décision soit fondée sur le traitement des *données à caractère personnel.* Si les décisions sont fondées sur quelque chose d'autre que les données à caractère personnel, l'article 22 du RGPD ne s'applique pas.

- Par conséquent, au lieu de faire en sorte que le SSAD demande des détails aux requérants (par exemple, des renseignements sur la personne concernée par la requête, comme le titulaire de nom de domaine, et pourquoi ses données sont requises), puis, en analysant ces informations (automatiquement) afin d'évaluer si les critères pertinents pour la diffusion des données d'enregistrement non publiques sont satisfaits, le SSAD pourrait plutôt publier les catégories de requêtes qui seront acceptées et demander aux requérants de confirmer qu'ils répondent aux critères pertinents. Dans ce cas, le SSAD ne traitera pas *les données à caractère personnel* sur la personne concernée par la requête afin de parvenir à une décision de divulgation des données – de sorte que l'article 22 ne s'appliquerait pas.

- Comme indiqué pour les questions précédentes, les parties impliquées dans le SSAD ont la responsabilité de prendre des « mesures techniques et organisationnelles appropriées » pour se protéger contre le risque d'utilisation abusive du système SSAD par les requérants.

- Toute décision de s'appuyer sur l'auto-certification, plutôt que sur l'évaluation des demandes, devrait donc être soigneusement équilibrée par rapport à ces obligations d'atténuation des risques. Cela permettrait probablement de réduire les occasions où cette approche d'auto-déclaration pourrait être utilisée. Bird & Bird note que, dans le cadre d'un tel programme, le SSAD pourrait toujours demander aux requérants de fournir des informations supplémentaires sur la nature de leur requête *à des fins d'audit*, mais elles ne seraient pas utilisées pour évaluer la requête elle-même (c'est-à-dire qu'elle ne serait pas utilisée pour la prise de décisions automatisées).

2. Question B

Dans cette question, **l'équipe responsable de l'EPDP demande des conseils sur la façon d'effectuer le test d'équilibrage selon l'article 6(1)(f) (en supposant qu'il n'est pas possible d'automatiser les étapes décrites).**

- Les directives officielles indiquent que le test d'équilibrage doit être divisé en quatre étapes :

    1. Évaluer l'intérêt auquel le traitement répond
    2. Prendre en compte l'impact sur la personne concernée
    3. Effectuer un test d'équilibrage provisoire
    4. Tenir compte de l'impact de toute protection supplémentaire déployée pour éviter tout impact injustifié sur la personne concernée.

1. Évaluer l'intérêt légitime de l'autorité de contrôle

- L'article 6(1)(f) dit que vous pouvez légalement procéder à un traitement si cela est « nécessaire aux fins des intérêts légitimes poursuivis par l'autorité de contrôle ou par un tiers ».
- Cela comprend trois sous-éléments : (i) la légitimité ; (ii) l'existence d'un intérêt ; et (iii) la nécessité.

Légitimité

- Il semble que la « légitimité » n'est pas une exigence difficile à satisfaire : le WP29 a déclaré *: «* un intérêt peut être considéré légitime si l'autorité de contrôle peut poursuivre cet intérêt conformément à la protection des données et à d'autres lois ».

Établissement de « l'intérêt » au traitement

- B&B a noté que si l'ICANN et les parties contractantes sont des responsables conjoints du traitement, elles doivent toutes deux établir un intérêt légitime dans le traitement. En ce qui concerne les parties contractantes, il est probable que l'intérêt pertinent soit celui du tiers, le requérant. L'ICANN, en revanche, peut être en mesure d'établir son intérêt à la sécurité, la stabilité et la résilience du système des noms de domaine ainsi que l'intérêt du requérant tiers ; et
- « Intérêt » n'équivaut pas à « finalité ».
    - La « finalité » est la raison spécifique pour laquelle les données sont traitées
    - L'« intérêt » est l'enjeu plus large qu'une autorité de contrôle peut avoir dans le traitement, ou l'avantage qu'il tire, ou que la société pourrait en tirer. (Cela signifie également que les intérêts peuvent être publics ou privés ; par exemple, dans le cas d'actions visant à prévenir la violation d'une marque, il peut y avoir

un intérêt privé pour la personne dont la marque a été violée et un intérêt public plus large pour prévenir un risque de confusion de la part du public. Ce facteur pourrait utilement être noté dans la documentation du test d'équilibrage).

- L'intérêt doit être « réel et spécifique », et non « vague et spéculatif ».
- À la page 25, le WP217 fournit une liste non exhaustive des contextes dans lesquels des intérêts légitimes pourraient survenir, notamment :
    - « l'exercice du droit à la liberté d'expression ou d'information, y compris dans les médias et les arts »
    - l'application des réclamations légales
    - la prévention de la fraude, la mauvaise utilisation des services,
    - la sécurité physique, informatique et du réseau
    - le traitement à des fins de recherche
- L'EPDP suggère que les garanties potentielles du SSAD pourraient inclure l'obligation pour le requérant de faire valoir qu'il a une base légale pour faire la demande et qu'il peut « démontrer sa base légale ». Toutefois, lorsque les données seront diffusées conformément à l'article 6(1)(f), il serait plus utile que le requérant confirme son *intérêt* à recevoir les données à caractère personnel.

Nécessité

- En ce qui concerne la nécessité, B&B conseille que le traitement proposé (divulgation) soit « nécessaire » pour cet intérêt.
    - Le cas du CEJU Oesterreichischer Rundfunk définit cela comme suit : *« … l'adjectif "nécessaire" […] implique qu'il s'agit d'un "besoin social urgent" et que la mesure employée est "proportionnelle à l'objectif légitime poursuivi".*
    - Une Cour d'appel britannique suggère également que nécessaire signifie « plus que souhaitable mais moins qu'indispensable ou absolument nécessaire ».
- B&B suggère qu'un facteur pertinent à prendre en considération pour la nécessité pourrait être la question de savoir si un requérant a tenté d'établir un contact avec la personne de toute autre manière (bien que cela puisse être inapproprié dans le cas de requêtes des forces de l'ordre).
- B&B note que le SSAD propose de demander aux requérants de confirmer qu'ils ne demandent que les données nécessaires à leur finalité.

2. Évaluer l'impact sur les personnes concernées

- B&B affirme que le CEPD suggère une série de facteurs à prendre en compte lors de l'évaluation de l'impact sur la personne concernée :
    - ***Évaluation de l'impact.*** Considérer l'impact direct sur les personnes concernées ainsi que des conséquences plus larges possibles du traitement des données (par exemple, déclenchement d'une procédure judiciaire).
    - ***Nature des données.*** Considérer le niveau de sensibilité des données et de la question de savoir si les données sont déjà accessibles au public.
    - ***Statut de la personne concernée.*** Déterminer si le statut de la personne concernée augmente sa vulnérabilité (par exemple, les enfants, d'autres classes protégées).
    - ***Portée du traitement.*** Déterminer si les données seront divulguées exclusivement au requérant (faible risque) ou rendues publiques, de sorte qu'elles seront accessibles à un grand nombre de personnes ou combinées à d'autres données (risque plus élevé).
    - ***Attentes raisonnables de la personne concernée***. Déterminer si la personne concernée s'attend raisonnablement à ce que ses données soient traitées/divulguées de cette manière.
    - ***Statut de l'autorité de contrôle et de la personne concernée.*** Examiner le pouvoir de négociation et tout déséquilibre d'autorité entre l'autorité de contrôle et la personne concernée.
- Il pourrait être possible pour le SSAD de tenir compte de ces facteurs, en identifiant les requêtes qui représenteraient un risque élevé pour les personnes concernées afin que ces requêtes reçoivent une attention supplémentaire.
- Une méthodologie classique du risque (qui examine la gravité et la probabilité) peut être utilisée pour évaluer le risque.
- Il ne s'agit pas d'un exercice purement quantitatif ; bien que les mesures associées à une requête (par exemple, le nombre de personnes concernées affectées) soient pertinentes, elles ne sont pas déterminantes. Un impact potentiellement significatif sur une seule personne concernée doit néanmoins être pris en compte.

3. Équilibre provisoire

- Une fois que les intérêts légitimes de l'autorité de contrôle ou du tiers et ceux de la personne concernée ont été pris en considération, ils peuvent être équilibrés. Garantir que les autres obligations de protection des données sont respectées contribue à l'équilibre mais n'est pas déterminant (par exemple, il est utile que le SSAD garantisse que des clauses contractuelles standard soient en place avec les requérants pour

assurer une protection adéquate des données, car cela pourrait réduire le risque pour les personnes, mais n'est pas déterminant).

4. Mesures de protection supplémentaires

- B&B déclare qu'il n'est pas clair comment l'équilibre devrait être atteint, l'autorité de contrôle peut envisager des mesures de protection supplémentaires pour réduire l'impact du traitement sur les personnes concernées.
- Cela comprend, par exemple :
    - Transparence
    - Renforcement les droits d'accès ou de port des données des personnes concernées
    - Droit inconditionnel de se désinscrire
- Le WP217, aux pages 41 et 42, fournit plus de détails sur les garanties qui peuvent aider à « faire pencher la balance » en faveur du traitement (ici, en faveur des divulgations), dans le cadre des tests d'équilibrage des intérêts légitimes.

Annexe : Question juridique 3 : intérêts légitimes et soumissions et/ou divulgations automatisées

a) supposant qu'il existe une politique qui permet aux parties accréditées d'accéder aux données WHOIS non publiques par le biais d'un système d'accès normalisé/de divulgation de données d'enregistrement de noms de domaine non publiques à des tiers (« SSAD ») (et exige que la partie accréditée s'engage à respecter certaines garanties raisonnables semblables à un code de conduite), est-il légalement admissible, en vertu de l'article 6(1)(f), de :

- définir des catégories spécifiques de requêtes émanant de parties accréditées (par exemple, réponse rapide à une attaque d'un logiciel malveillant ou contacter avec un contrevenant IP non réactif), pour lesquelles il pourrait y avoir des soumissions automatisées pour des données WHOIS non publiques, sans avoir à vérifier manuellement les qualifications des parties accréditées pour chaque requête de divulgation individuelle, et/ou

- permettre la divulgation automatisée de ces données, sans nécessiter un examen manuel par l'autorité de contrôle ou le traiteur de chaque demande de divulgation individuelle.

b) En outre, s'il n'était pas possible d'automatiser l'une de ces étapes, veuillez fournir des directives sur la façon d'effectuer le test d'équilibrage en vertu de l'article 6(1)(f).

À titre de référence, veuillez vous reporter aux mesures de protection possibles suivantes :

- la divulgation est requise dans le cadre du contrat des CP avec l'ICANN (résultant de la politique de l'étape 2 de l'EPDP).
- Le contrat des CP avec l'ICANN exige que les CP notifient la personne concernée des finalités pour lesquelles, et les types d'entités par lesquelles, les données à caractère personnel peuvent être traitées. la CP est tenue d'informer la personne concernée de cette possibilité de s'exclure avant que la personne concernée ne conclue un contrat d'enregistrement avec la CP, et à nouveau annuellement par le biais du rappel d'exactitude des données d'enregistrement exigé par l'ICANN. La partie contractante l'a fait.
- L'ICANN ou son délégué ont validé l'identité du requérant et ont exigé que le requérant :
  - démontre qu'il se fonde sur une base légitime pour demander et traiter les données,
  - présente son fondement légitime,
  - indique qu'il ne demande que les données nécessaires à sa finalité,

- accepte de traiter les données conformément au RGPD, et
- accepte les clauses contractuelles standard pour le transfert de données.

- L'ICANN ou son délégué consigne les requêtes de données d'enregistrement non publiques, vérifie régulièrement ces journaux, prend des mesures de conformité contre les abus présumés et met ces journaux à disposition sur demande de la personne concernée.

Question 4

Résumé analytique :

L'équipe responsable de l'étape 2 de l'EPDP a envoyé sa première série de questions à Bird & Bird le 29 août 2019. Bird & Bird a répondu à ce lot de questions dans une série de trois notes. La note 3 a été présentée le 9 septembre 2019 et analyse les questions relatives aux bases juridiques selon lesquelles les données à caractère personnel contenues dans les données d'enregistrement de gTLD pourraient être divulguées aux organismes d'application de la loi en dehors de la juridiction de l'autorité de contrôle des données.

Plus précisément, la note répond aux questions suivantes :

- Une autorité de contrôle peut-elle se fonder sur l'article 6(1)(c) du RGPD pour divulguer des données à caractère personnel aux autorités responsables de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ?
- Si ce n'est pas le cas, l'autorité de contrôle peut-elle se fonder sur d'autres bases juridiques, outre l'article 6(1), pour divulguer des données à caractère personnel aux autorités responsables de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ?
- Est-il possible pour les autorités chargées de l'application de la loi non basées dans l'UE de s'appuyer sur l'article 6(1)(f) du RGPD comme base juridique pour leur traitement ? Dans ce contexte, l'autorité de contrôle de données peut-elle se fonder sur l'article 6(1)(f) du RGPD pour divulguer les données à caractère personnel ? Si les autorités chargées de l'application de la loi non basées dans l'UE ne peuvent pas se fonder sur l'article 6(1)(f) du RGPD comme base juridique pour leur traitement, sur quelle base peuvent-elles s'appuyer ?

Dans l'ensemble, Bird & Bird a indiqué que :

1. Pour appliquer l'article 6(1)(c), l'autorité de contrôle doit être assujettie au « droit de l'Union ou à la législation d'un État membre » et ce motif a donc une application limitée

lorsque l'autorité d'application de la loi est en dehors de la juridiction de l'autorité de contrôle.

2. En vertu des six bases légitimes pour le traitement des données à caractère personnel, les articles 6(1)(a) - consentement, l'article 6(1)b) - Contrat, l'article 6(1)(d) - intérêts vitaux d'une personne et l'article 6(1)(e) - intérêt public ou autorité officielle ne s'appliquent vraisemblablement pas aux requêtes des autorités d'application de la loi.
3. Art 6(1)(f) - l'intérêt légitime peut constituer une base applicable pour l'autorité de contrôle lorsqu'une autorité chargée de l'application de la loi qui n'appartient pas à l'UE demande à obtenir des données à caractère personnel d'une autorité de contrôle de l'UE.
4. Si une autorité d'application de la loi se trouve en dehors de l'EEE, sa base juridique pour le traitement en vertu du RGPD n'est pas pertinente car elle ne sera pas assujettie au RGPD. Les organisations qui divulguent des informations aux autorités d'application de la loi en dehors de l'EEE auront toujours besoin d'une base valide pour le faire, ce qui sera généralement un intérêt légitime dans le cas de l'ICANN.
5. Lorsque le CP est soumis au RGPD mais qu'il est situé en dehors de l'EEE, il est également soumis à la législation locale. Cela signifie que les autorités de contrôle peuvent être confrontées à un conflit de lois.

1. Une autorité de contrôle peut-elle se fonder sur l'article 6(1)(c) du RGPD pour divulguer des données à caractère personnel aux autorités responsables de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ?

- Le traitement nécessaire au respect d'une obligation légale à laquelle l'autorité de contrôle est assujettie n'est disponible que lorsque l'obligation légale est définie dans le droit de l'UE ou de l'État membre.

- Lorsque l'autorité de contrôle est soumise à des obligations de divulgation découlant des lois en vigueur dans des juridictions en dehors de l'UE, elle ne peut pas se fonder sur à l'article 6(1)(c).

- L'autorité de contrôle peut être soumise à l'obligation légale, en vertu de la législation de l'UE ou des États membres, de divulguer des données à caractère personnel à une autorité d'application de la loi non européenne.

- Les traités d'assistance juridique mutuelle (MLAT) peuvent s'appliquer, mais lorsqu'une requête survient alors qu'il existe un MLAT, l'autorité de contrôle doit refuser la demande et se référer au MLAT. En l'absence d'un accord, MLAT ou autre, l'autorité de contrôle doit s'assurer que la divulgation dans un pays tiers ne constitue pas une violation de la législation locale.

2. L'autorité de contrôle peut-elle se fonder sur d'autres bases juridiques, outre l'article 6(1)(f) du RGPD, pour divulguer des données à caractère personnel aux autorités responsables de l'application de la loi en dehors de la juridiction de l'autorité de contrôle ?

- Les articles 6(1)(f) et 6(1)(c) peuvent s'appliquer, mais les cinq autres bases légales pour le traitement des données à caractère personnel ne s'appliquent probablement pas.

- Lorsqu'une autorité d'application de la loi en dehors de l'UE requiert d'obtenir des données à caractère personnel d'une autorité de contrôle de l'UE, l'autorité de contrôle peut être en mesure de montrer un intérêt légitime à divulguer les données (en vertu de l'article 6(1)(f)). Le CEPD a également suggéré cette approche dans la correspondance avec l'ICANN (par exemple EDPB-85-2018).

3. Est-il possible pour les autorités chargées de l'application de la loi non basées dans l'UE de s'appuyer sur l'article 6(1)(f) du RGPD comme base juridique pour leur traitement ? Dans ce contexte, l'autorité de contrôle de données peut-elle se fonder sur l'article 6(1)(f) du RGPD pour divulguer les données à caractère personnel ? Si les autorités chargées de l'application de la loi non basées dans l'UE ne peuvent pas se fonder sur l'article 6(1)(f) du RGPD comme base juridique pour leur traitement, sur quelle base peuvent-elles s'appuyer ?

- En tant qu'entités d'un pays, les autorités d'application de la loi sont couvertes par l'immunité de l'État et, par conséquent, les autorités d'application de la loi non basées dans l'UE ne sont pas assujetties au RGPD.

- Même en supposant que le RGPD puisse s'appliquer aux autorités d'application de la loi non basées dans l'UE, il semble peu probable que les autorités d'application de la loi en dehors de l'UE envisagent de justifier leur traitement aux termes du RGPD.

- Les autorités d'application de la loi non basées dans l'UE n'ont donc pas besoin d'évaluer sur quelle base juridique du RGPD elles se fondent pour le traitement des données.

- Une autorité de contrôle qui transfère des données à une autorité d'application de la loi en dehors de l'UE devra néanmoins chercher la manière de respecter les obligations du chapitre V (transferts de données à caractère personnel vers des pays tiers ou des organisations internationales).

Question 5 (adresses e-mail pseudonymisées)

Le groupe a discuté de la possibilité de remplacer l'adresse de courrier électronique fournie par la personne concernée par une autre adresse qui ne permettrait pas d'identifier la personne concernée (exemple : 'sfjgsdfsafgkas@pseudo.nym'). Avec cette approche, deux options ont été soulevées dans la discussion, où (a) la même chaîne unique serait utilisée pour plusieurs enregistrements par la personne concernée (« pseudonymisation »), ou (b) la chaîne serait unique pour chaque enregistrement (« anonymisation »). Dans l'option (a), l'identité de la personne concernée par les données peut, mais ne doit pas nécessairement, devenir identifiable en faisant référence au contenu de tous les enregistrements de noms de domaine pour lesquels la chaîne est utilisée.

À partir de ces options, la question suivante s'est posée : Sous les options (a) et/ou (b), l'adresse alternative devrait-elle être considérée comme des données à caractère personnel de la personne concernée en vertu du RGPD ? Quelles seraient les conséquences juridiques et les risques de cette détermination en ce qui concerne la publication proposée de cette chaîne dans la partie accessible au public du service d'annuaire de données d'enregistrement (RDS) ?

Réponse sommaire de Bird & Bird

Nous croyons que l'option ((a) ou (b)) serait toujours interprétée comme la publication de données à caractère personnel sur le Web. Cela semblerait couvert par une déclaration faite dans l'avis de 2014 du Groupe de travail Article 29 sur les techniques d'anonymisation [ec.europa.eu] : « Lorsqu'une autorité de contrôle de données ne supprime pas les données d'origine (identifiables) au niveau de l'événement et que l'autorité de contrôle de données remet une partie de cet ensemble de données (par exemple après suppression ou masquage de données identifiables), l'ensemble des données résultantes reste des données à caractère personnel ». L'objectif de la mise à disposition de cette adresse e-mail, même si elle est masquée, est probablement de permettre aux tiers de contacter directement la personne concernée (par exemple, pour la notifier des convocations judiciaires, lui exiger des mises en possession, etc.), de sorte qu'elle soit clairement liée à cette personne concernée particulière, du moins en ce qui concerne l'ICANN et les parties contractantes. Cependant, l'une ou l'autre option serait considérée comme une technologie d'amélioration de la confidentialité (OPET) / une mesure de respect de la vie privée dès la conception.

Question 6 (Consentement)

Les données d'enregistrement soumises par les titulaires de noms de domaine étant des personnes morales peuvent contenir les données de personnes physiques. Une note de l'étape 1 indiquait que les titulaires de noms de domaine peuvent se fier de l'auto-identification d'un titulaire comme personne morale ou physique si le risque est atténué en prenant d'autres mesures pour assurer l'exactitude de la désignation du titulaire de nom de domaine. À titre de suivi de cette note de service : quelles sont les options et les exigences de consentement liées à de telles désignations ? Plus précisément : les autorités de contrôle de données ont-elles le droit de se fier à une déclaration obligeant les titulaires étant des personnes morales à obtenir le consentement d'une personne physique qui agirait comme contact et dont les informations peuvent être affichées publiquement dans le RDS ? Si oui, le cas échéant, quelles représentations serait-il utile d'obtenir, de la part de l'autorité de contrôle, du titulaire de nom de domaine étant une personne morale inscrite dans ce cas ?

Dans le cadre de votre analyse, veuillez consulter les politiques et les pratiques du registre du protocole Internet (adresse IP) RIPE-NCC (le registre pour l'Europe, basé aux Pays-Bas). Les clients de RIPE-NCC (titulaires de noms de domaine) sont des personnes morales dont les données sont affichées publiquement dans le WHOIS. RIPE-NCC tient les titulaires de noms de domaine étant des personnes morales responsables d'obtenir la permission de ces personnes physiques et fournit des procédures et des garanties à cet égard. RIPE-NCC énonce des justifications de mission et des finalités pour la collecte de données similaires à celles de la Spécification temporaire de l'ICANN. Des politiques et des procédures similaires pourraient-elles être utilisées à l'ICANN ?

Voir aussi les politiques d'ARIN, le registre d'adresses IP pour l'Amérique du Nord. ARIN a quelques clients situés dans l'UE. ARIN publie également les données sur les personnes physiques dans ses résultats WHOIS. Les clients d'ARIN sont des personnes physiques qui soumettent les données des contacts de personnes physiques.

Réponse sommaire de Bird & Bird

Le présent document analyse les exigences de consentement énoncées dans le RGPD et examine les options de consentement aux fins de la publication dans le RDS des données à caractère personnel fournies dans le contexte de l'enregistrement des titulaires de noms de domaine étant des personnes morales.

Exigences de consentement

Conformément au RGPD, le consentement doit être donné librement, précis, informé et sans ambiguïté. Il doit également être obtenu avant le traitement. Les autorités de contrôle doivent pouvoir démontrer qu'un consentement valide ait été donné et que les personnes aient le droit de retirer leur consentement à tout moment. En vertu du RGPD, l'obligation d'obtenir le

consentement incombe à l'autorité de contrôle. L'autorité de contrôle peut demander à un tiers d'obtenir le consentement de personnes en son nom ; toutefois, cela ne libérera pas l'autorité de contrôle de ses obligations aux termes du RGPD.

Options de consentement

Sur la base des exigences ci-dessus, le présent document examine les options suivantes d'obtention du consentement pour rendre les données à caractère personnel publiques dans le RDS et énonce les considérations de conformité de chaque option :

1. Les autorités de contrôle demandent un consentement valide directement auprès des personnes concernées
    - La diffusion de données à caractère personnel dans le RDS est facultative.
    - Avant de rendre les données à caractère personnel publiques, l'autorité de contrôle communique directement avec les personnes pour obtenir leur consentement conformément au RGPD.
    - En cas de refus du consentement ou de non-réponse, les données à caractère personnel ne seront pas rendues publiques.

2. Le titulaire de nom de domaine obtient un consentement valide et en fournit une preuve à l'autorité de contrôle
    - La diffusion de données à caractère personnel dans le RDS est facultative.
    - Avant de rendre publiques les données à caractère personnel, l'autorité de contrôle exige que le titulaire de nom de domaine : a) obtienne le consentement des personnes ; b) fournisse à l'autorité de contrôle la preuve que le consentement a été obtenu.
    - En cas de refus de consentement ou de non-réception de preuves, les données à caractère personnel ne seront pas rendues publiques

3. Le titulaire de nom de domaine obtient un consentement valide et l'autorité de contrôle le confirme avec la personne
    - Avant de rendre publiques les données à caractère personnel, l'autorité de contrôle exige que le titulaire de nom de domaine : a) obtienne le consentement des personnes ; b) fournisse à l'autorité de contrôle la preuve que le consentement a été obtenu.
    - L'autorité de contrôle assure un suivi direct avec la personne : elle les informe que le titulaire de nom de domaine a confirmé qu'il a accordé son consentement.

4. Le titulaire de nom de domaine s'engage à obtenir le consentement
    - Les titulaires de noms de domaine sont autorisés à fournir des informations de contact non personnelles.
    - Les données d'enregistrement sont rendues publiques par défaut (peu importe si les données à caractère personnel sont incluses ou non).

- Au moyen d'une déclaration, les titulaires de noms de domaine s'engagent à s'assurer qu'ils ont obtenu le consentement des personnes s'ils choisissent de fournir des données à caractère personnel.

Question 7 (exactitude)

Question 1a

Qui a la capacité d'invoquer le principe de l'exactitude ? Nous comprenons que le principe de l'exactitude vise à protéger la personne concernée contre les dommages résultant du traitement d'informations inexactes. D'autres, comme les parties contractantes et l'ICANN (en tant qu'autorités de contrôle), les autorités d'application de la loi, les titulaires de droits de propriété intellectuelle, etc., ont-ils le droit d'invoquer le principe de l'exactitude dan le cadre du RGPD ? En répondant à cette question, nous vous prions de préciser les parties/intérêts que nous devrions prendre en compte en général, et plus particulièrement lors de l'interprétation des passages suivants des notes précédentes :

- Les deux notes font référence aux « parties pertinentes » dans plusieurs sections. Les « parties pertinentes » sont-elles limitées au(x) autorité(s) de contrôle ou devrions-nous rendre compte également des intérêts de tiers ?
    - « Il peut y avoir des questions quant au fait de savoir s'il suffit que le titulaire de nom enregistré (RNH) ou le titulaire du compte confirme l'exactitude des informations relatives aux contacts techniques et administratifs, au lieu de demander directement des informations sur ces contacts. Le RGPD n'exige pas nécessairement que, dans les cas où les données à caractère personnel doivent être validées, elles soient validées par la personne elle-même. L'ICANN et les parties concernées peuvent compter sur des tiers pour confirmer l'exactitude des données à caractère personnel s'il est raisonnable de le faire. Nous ne voyons donc pas de raison immédiate pour déclarer insuffisantes les procédures actuelles ». (accent d'intensité ajouté) (paragraphe 19 – exactitude)
    - « En somme, étant donné que le respect du principe de l'exactitude est fondé sur une norme de raisonnabilité, l'ICANN et les parties concernées seront mieux placées pour évaluer si ces procédures sont suffisantes. De notre point de vue, comme les procédures exigent des mesures affirmatives qui aideront à confirmer l'exactitude, à moins qu'il n'y ait des raisons pour croire qu'elles sont insuffisantes, nous ne voyons pas clairement la nécessité de les examiner ». (accent d'intensité ajouté) (paragraphe 21 - exactitude)
    - « Si les parties pertinentes n'avaient aucune raison pour douter de la fiabilité de l'auto-identification d'un titulaire de nom de domaine, elles pourraient alors compter sur l'auto-identification seule, sans confirmation indépendante. Toutefois, nous comprenons que les parties s'inquiètent du fait que certains titulaires de noms de domaine ne comprendront pas la question et s'auto-identifieront à tort. Par conséquent, il y aurait un risque de responsabilité si les parties pertinentes ne prenaient pas d'autres mesures pour garantir l'exactitude de la désignation du titulaire de nom de domaine ». (accent d'intensité ajouté) (paragraphe 17 – personne morale vs personne physique)

1.b De même, la note concernant la personne morale et la personne physique fait référence à l'« importance » des données pour déterminer le niveau d'effort requis pour assurer l'exactitude. L'évaluation de l'« importance » des données se limite-t-elle à la prise en compte de l'importance pour la personne concernée et la ou les autorités(s) de contrôle, ou inclut-elle également l'importance des données pour les tiers (dans ce cas, les autorités d'application de la loi, les titulaires de droits de propriété intellectuelle, et d'autres personnes qui demanderaient les données au contrôleur pour leurs propres finalités) ?

- Comme expliqué dans les directives de l'ICO, « plus il est important que les données à caractère personnel soient exactes, plus vous devez déployer d'efforts pour en assurer l'exactitude. Ainsi, si vous utilisez les données pour prendre des décisions qui peuvent affecter de manière significative la personne concernée ou d'autres, vous devez faire plus d'efforts pour en garantir l'exactitude ». (paragraphe 14 – personne morale vs personne physique)

Résumé analytique de Bird & Bird

Le présent document examine d'autres considérations relatives au principe de l'exactitude (les parties ayant l'obligation de se conformer à ce principe, les personnes qui ont le pouvoir de l'invoquer et la base sur laquelle l'exactitude des données doit être évaluée). Il définit les facteurs à prendre en considération lors de l'évaluation de l'exactitude des données et formule des recommandations sur les mesures visant à améliorer l'exactitude des données d'enregistrement détenues par les parties contractantes.

Parties assujetties au principe de l'exactitude et « parties pertinentes »

L'obligation de se conformer au principe de l'exactitude du RGPD incombe au(x) autorité(s) de contrôle. Les références aux « parties pertinentes » dans les notes concernant l'exactitude et la distinction entre personne morale et personne physique faisaient allusion à la ou les autorité/s de contrôle pertinente/s des données WHOIS.

Parties ayant le droit d'invoquer le principe de l'exactitude

Le RGPD prévoit une gamme de recours : plaintes aux autorités de surveillance, recours judiciaires et droit à l'indemnisation d'une autorité de contrôle ou d'un traiteur. Les personnes concernées (et, lorsque la législation nationale le permet, leurs représentants) ont le droit d'exercer tous les recours prévus dans le RGPD. Dans certains cas, ces droits peuvent également être exercés par d'autres personnes, physiques ou morales, par exemple, celles qui sont touchées par les décisions d'une autorité de surveillance ou celles qui ont subi des dommages à la suite d'une infraction au RGPD.

Intérêts des différentes parties en matière d'exactitude

Le but pour lequel les données à caractère personnel sont traitées est pertinent pour déterminer les mesures nécessaires pour assurer l'exactitude des données. Les intérêts de la personne concernée doivent être pris en compte au moment d'évaluer l'exactitude des données. Dans certaines circonstances, les intérêts de l'autorité de contrôle seront également pertinents. Bien qu'il y ait quelques références aux droits des « autres » dans les directrices de l'ICO sur l'exactitude, ce point n'est pas encore éclairé dans notre examen des directives, de la jurisprudence ou de la bibliographie. Étant donné le manque d'orientation, nous ne recommandons pas de mettre trop l'accent sur ce point.

Mesures raisonnables pour l'exactitude des données

Le principe de l'exactitude n'a pas été examiné de façon approfondie dans la bibliographie et la jurisprudence et les références à ce principe sont limitées. Le caractère raisonnable et approprié des mesures d'exactitude devrait être pris en considération à la lumière de l'approche axée sur les risques du RGPD, en tenant compte, entre autres, de la finalité et de l'incidence du traitement. Une liste des mesures d'exactitude suggérées est présentée dans ce document.

Question 8 (cas d'utilisation de l'automatisation)

Contexte

1. Dans le premier scénario, l'automatisation serait effectuée au sein d'une passerelle centrale chargée de recevoir les requêtes des utilisateurs accrédités. La passerelle centrale ferait une recommandation automatisée pour savoir si les données requises devraient être divulguées ou non, tandis que la décision finale de divulguer les données incomberait aux parties contractantes, qui pourraient suivre ou non la recommandation (scénario 1.a.). Les parties contractantes qui font suffisamment confiance à la passerelle peuvent choisir d'automatiser la décision de divulguer les données (scénario 1.b.).

2. Dans le deuxième scénario, la décision de divulguer les données du titulaire de nom de domaine serait prise par la passerelle centrale sans que la partie contractante soit en mesure d'examiner la requête. La passerelle centrale prendrait cette décision soit (i) après avoir obtenu les données pertinentes de la partie contractante et après avoir évalué les données dans le cadre de sa prise de décision (scénario 2.a.), ou (ii) sans obtenir les données du titulaire de nom de domaine (auquel cas, la décision serait fondée uniquement sur les renseignements concernant le requérant et les affirmations faites dans la requête) (scénario 2.b.). Un exemple de ce dernier scénario serait la divulgation automatisée des données d'enregistrement pour microsoft-login.com au propriétaire vérifié de la marque déposée MICROSOFT en réponse à une requête alléguant une atteinte à la marque et alléguant l'intention de traiter les données pour l'établissement, l'exercice ou la défense de revendications juridiques. On nous a demandé de supposer que chaque scénario ferait l'objet d'une série de garanties qui sont incluses dans la présente note en tant qu'annexe 1.

A. Cas d'utilisation dans le scénario 1 :

À la lumière des conseils fournis précédemment dans les notes sur les questions 1 et 2 (responsabilité) et la question 3 (automatisation), veuillez fournir l'analyse suivante pour chaque cas d'utilisation dans la Pièce 1 :

1. Veuillez décrire le risque de responsabilité pour la passerelle centrale et pour les parties contractantes (« CP ») lié à l'automatisation de cette recommandation et à l'automatisation de la décision de divulguer des informations personnelles à un tiers. Si des renseignements supplémentaires sont nécessaires pour évaluer le risque, veuillez prendre note des renseignements supplémentaires nécessaires.

2. La décision de divulguer des informations personnelles à un tiers est-elle une décision « qui entraîne des effets juridiques concernant [la personne concernée] ou qui l'affecte de façon tout aussi significative » dans le cadre de l'article 22 ?

3. Existe-t-il des mesures ou des garanties supplémentaires qui atténueraient le risque de responsabilité ?

4. La prise de décisions automatisée effectuée de cette manière a-t-elle un impact sur votre analyse des rôles/responsabilités des parties décrites dans la note concernant les questions 1 et 2 (par exemple, les parties contractantes restent des autorités de contrôle responsables lorsque « la divulgation a lieu de manière automatisée, sans intervention manuelle ». 1.1.4).

B. Cas d'utilisation dans le scénario 2 :

Dans le deuxième scénario -alternatif-, où la passerelle centrale aurait la capacité contractuelle d'exiger aux parties contractantes qu'elles lui fournissent les données :

1. Quel serait l'impact des scénarios alternatifs sur l'analyse fournie aux questions 1 à 4 ci-dessus ?

2. Quel scénario implique le moins de risque de responsabilité pour les parties contractantes ? Pour y répondre, veuillez indiquer vos hypothèses concernant les rôles respectifs de l'ICANN et des parties contractantes, y compris un scénario dans lequel la passerelle centralisée aurait externalisé la prise de décisions à un prestataire de services juridiques indépendant.

C. Précisions supplémentaires sur l'automatisation

1. Si la décision de divulguer des données à caractère personnel à un tiers est automatisée, de quelle manière la ou les autorité/s de contrôle devraient-elles fournir au titulaire de nom de domaine des informations concernant la possibilité d'une prise de décisions automatisée dans le traitement de ses renseignements personnels ? Comment ces informations devraient-elles être communiquées au titulaire de nom de domaine et quelles informations relatives à la prise de décisions automatisée devraient-elles être communiquées au titulaire de nom de domaine afin d'assurer un traitement juste et transparent conformément à l'article 13 ?

2. La fourniture des renseignements énoncés dans la réponse à la question C.1 ci-dessus par la ou les autorité/s de contrôle a-t-elle une incidence sur le droit du titulaire de nom de domaine d'obtenir une confirmation quant à l'automatisation de la prise de la décision de divulguer ou non ses informations personnelles à un tiers ? Cela affecte-t-il le droit du titulaire de nom de domaine d'obtenir des informations pertinentes associées, conformément à l'article 15.1(h) ?

3. La manière dont la prise de la décisions est décrite ci-dessus a-t-elle une incidence sur la façon dont ces informations doivent être fournies ?

4. Quel rôle la cause immédiate joue-t-elle dans la détermination d'un effet juridique ou tout aussi significatif qu'engagerait une décision de divulgation (c'est-à-dire, quel degré de rapport doit-il y avoir entre la décision de divulguer les données à caractère personnel d'un titulaire de

nom de domaine et l'effet juridique ou tout aussi significatif du traitement des données à caractère personnel) ? Veuillez décrire le risque de responsabilité envers la passerelle centrale ou la partie contractante si, après avoir reçu des données à caractère personnel, le requérant entreprend son propre traitement, qui a un effet légal ou tout aussi significatif.

5. Dans la section 1.12 de la note précédente sur l'automatisation, Bird & Bird a déclaré : Il peut également être possible de structurer le SSAD de sorte qu'il n'implique pas « une décision fondée uniquement sur un traitement automatisé ». Pour plus de détails, au lieu de faire que le SSAD demande des renseignements aux requérants et évalue si les critères pertinents pour la divulgation des données d'enregistrement non publiques sont satisfaits, le SSAD pourrait publier les catégories de demandes qui seront acceptées et demander aux requérants de confirmer qu'ils satisfont aux critères pertinents. Dans ce cas, il n'y aurait pas de traitement automatisé qui conduise à la décision de divulguer les données. Le SSAD pourrait demander aux requérants d'apporter des informations supplémentaires sur la nature de leur requête aux fins de la vérification, mais elles ne seraient pas utilisées pour évaluer la requête elle-même. Pourriez-vous nous expliquer comment (i) la publication des catégories de demandes qui seront approuvées et (ii) l'obligation pour un requérant de sélectionner manuellement la catégorie applicable et de confirmer qu'il répond aux critères de cette catégorie de demandes entraînerait la décision d'une divulgation « non automatisée » ?

Résumé analytique de Bird & Bird

Le présent document examine les scénarios et les cas d'utilisation présentés par l'équipe responsable de l'EPDP en ce qui concerne les décisions automatisées de divulgation des données non publiques des titulaires de noms de domaine. Il identifie les cas de décisions entièrement automatisées qui relèvent de l'article 22 du RGPD, les enjeux associés à l'article 22 et les solutions de rechange disponibles. Par ailleurs, le document propose des mesures de protection des données et examine les considérations de transparence dans le contexte du SSAD. Enfin, il examine le statut des parties dans chaque scénario et le risque de responsabilité associé.

Décisions et alternatives à l'article 22

L'article 22 du RGPD s'applique aux décisions entièrement automatisées qui entraînent des effets juridiques ou tout aussi significatifs. Aux termes de l'article 22, les décisions ne sont admises que dans des cas limités, qui ne sont pas susceptibles de s'appliquer au contexte du SSAD. Les décisions entièrement automatisées ne seront autorisées que si elles : (a) n'incluent pas le traitement des données à caractère personnel; (b) n'entraînent pas d'effets juridiques ou tout aussi significatifs ; (c) sont autorisées par la législation applicable de l'UE ou de l'État membre pertinent qui prévoit des mesures appropriées pour protéger les personnes ; ou (d) sont couverts par une dérogation nationale de l'article 22 (par exemple, aux fins de la détection d'infractions pénales). Dans tous les autres cas, il faut une participation humaine significative au processus de prise de décisions.

Les critères de l'article 22 s'appliquent-ils au SSAD ?

(A) traitement automatisé exclusivement : pour que l'article 22 s'applique, il doit y avoir un certain traitement des données à caractère personnel, mais il n'est pas obligatoire que seules les données à caractère personnel soient traitées pour la prise de la décisions. La décision examinée ici impliquera dans la plupart des cas le traitement des données à caractère personnel ; ce sera le cas, que la passerelle centrale ait ou non accès aux données requises et tienne ou pas compte de ces données dans la prise de la décisions. À l'exception du scénario 1.a, où le SSAD ne ferait qu'émettre une recommandation automatisée, tous les autres scénarios incluraient la prise d'une décision (de divulguer les données des titulaires de noms de domaine à des tiers) fondée uniquement sur le traitement automatisé.

(b) Effet juridique ou tout aussi significatif : le terme n'est pas défini dans le RGPD ; toutefois, il indique un seuil élevé. La question de savoir si la divulgation des données du titulaire de nom de domaine a un tel effet dépendra des circonstances de la requête : le document évalue la nature des effets de la divulgation dans chaque cas d'utilisation. Nous avons donné des réponses claires affirmatives ou négatives lorsque cela était possible : certains cas d'utilisation exigeraient une discussion plus approfondie. Le rôle de la cause immédiate dans la détermination des effets d'une décision n'a pas été examiné par les tribunaux ou les autorités de surveillance. Il y a un certain débat dans la bibliographie allemande ; cependant, au vu de l'absence d'une discussion plus généralisée, il pourrait être utile de connaître l'avis des autorités de surveillance sur ce sujet, car cela pourrait permettre d'automatiser le SSAD sur la base que la passerelle centrale/les CP ne prennent qu'une décision préparatoire.

Garanties

Une liste des mesures de protection des données suggérées figure à l'annexe 2 du présent document. Cela comprend entre autres : travailler en liaison avec les autorités de surveillance, définir clairement chaque cas d'utilisation et établir une base juridique, imposer des conditions de divulgation appropriées au requérant, mettre en œuvre des mesures de sécurité appropriées, prendre des mesures pour se conformer au principe de la responsabilité, établir des politiques pour satisfaire les droits des personnes et conclure des accords de protection des données appropriées avec les traiteurs.

Transparence

La façon de fournir les informations n'est pas affectée par l'existence d'une prise de décisions automatisée, mais le contenu de l'information l'est.

- L'information sera généralement fournie à travers un avis de confidentialité ; étant donnée l'importance du SSAD pour le système des noms de domaine, il serait approprié de la présenter d'une manière bien visible.

- Il serait plus efficace pour les bureaux d'enregistrement de fournir les informations pertinentes (compte tenu de leur relation directe avec les titulaires de noms de domaine), qu'ils ne soient pas considérés comme des autorités de contrôle dans le contexte du SSAD. S'ils ne sont pas des autorités de contrôle, mais fournissent l'information au nom de celle-ci, les titulaires de noms de domaine devraient être clairement informés.
- En ce qui concerne le contenu, pour les décisions en vertu de l'article 22 uniquement, l'avis doit également inclure des informations sur : l'existence d'une décision automatisée, la logique en cause et l'importance et les conséquences envisagées du traitement.
- Les éléments de l'article 15 du RGPD (droit d'accès) doivent être fournis sur demande même s'ils ont déjà été inclus dans l'avis.
- Le droit d'accès exige que les autorités de contrôle fournissent des informations sur les destinataires auxquels les données « ont été ou seront divulguées » : cela indique qu'en l'absence d'exemptions applicables, les titulaires de noms de domaine exerçant leur droit d'accès doivent être informés de la divulgation de leurs données à des tiers.

Statut des parties

(a) Dans le scénario 1, la décision ultime de divulguer les données des titulaires de noms de domaine incombe aux CP. L'analyse effectuée dans la note relative à la responsabilité s'appliquerait également ici et le plus probable serait que les CP soient considérées par les autorités de surveillance comme des responsables conjoints du traitement avec l'ICANN.

(b) Dans le scénario 2, la situation est moins claire. Selon qu'une approche généralisée ou détaillée soit adoptée, les CP peuvent être des autorités de contrôle (ou responsables conjoints du traitement) pour la prise de la décision automatisée et la divulgation de données aux requérants ou simplement pour la divulgation de données à la passerelle centrale. Nous croyons que la deuxième option (des autorités de contrôle exclusivement pour la divulgation des données à la passerelle centrale) est la meilleure analyse, mais le point n'est pas clair. Il est peu probable que l'externalisation de la prise de la décision à un prestataire de services juridiques indépendant modifie la position ci-dessus.

Il ne serait pas viable de soutenir que les CP sont des traiteurs dans aucun des deux scénarios.

La responsabilité des CP est examinée en ce qui concerne :

(a) le statut des CP : lorsque les CP sont des responsables conjoints du traitement, il est important d'attribuer clairement les tâches et les responsabilités à travers un contrat ;
(b) le type de responsabilité :

- responsabilité envers les personnes : la responsabilité conjointe et solidaire est la norme et les CP peuvent être tenues responsables de l'ensemble des dommages

provoqués par le traitement auquel elles sont impliquées, indépendamment de leur statut. Elles ne peuvent éviter cela qu'en démontrant qu'elles n'étaient pas impliquées dans l'événement donnant lieu aux dommages. Autrement, elles ont le droit de réclamer aux autres autorités responsables du contrôle la partie de l'indemnisation correspondant à leur responsabilité.

- La responsabilité envers les autorités de surveillance : la responsabilité conjointe et solidaire est moins claire ici et il y a lieu de soutenir que l'action d'exécution devrait être imposée sur la base du « degré de responsabilité » de chaque partie.

En termes de risques, le scénario 2 semble présenter un risque de responsabilité moindre tant en ce qui concerne l'indemnisation des personnes qu'en ce qui concerne les mesures d'exécution par les autorités de surveillance.