



Guide pour l'examen de la licéité de la communication transfrontière de données (art. 16, al. 2, let. b et d, LPD)

(publié en juin 2021, adapté à la LPD révisée en mai 2023)

1. But du guide

Le présent guide vise à faciliter l'examen – par les personnes qui traitent des données – de la licéité du transfert de données à caractère personnel vers l'étranger.

Il illustre, au moyen d'un schéma, la procédure de transfert de données vers l'étranger dans les cas où le pays concerné ne dispose pas d'une législation qui assure un niveau de protection adéquat et où cette carence doit être compensée par des garanties suffisantes (art. 16, al. 2, let. b et d, LPD et art. 9, al. 3, de l'ordonnance relative à la loi fédérale sur la protection des données, OPDo, RS 235.11, du 31 août 2022). Précisons que le présent guide n'aborde pas les conditions énoncées à l'art. 16, al. 2, let. a, c et e, et art. 17 LPD.

RS 235.1 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), art. 16 al. 2, let. b et d)

Chapitre 3 Communication de données personnelles à l'étranger

Art. 16 Principes

¹ Des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat ou qu'un organisme international garantit un niveau de protection adéquat.

² En l'absence d'une décision du Conseil fédéral au sens de l'al. 1, des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti par:

[...]

b. les clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son cocontractant, préalablement communiquées au PFPDT;

[...]

d. des clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT;

[...]

RS 235.11 Ordonnance du 31 août 2022 relative à la loi fédérale sur la protection des données (OPDo), Art. 9

Art. 9 Clauses de protection des données d'un contrat et garanties spécifiques

¹ Les clauses de protection des données d'un contrat au sens de l'art. 16, al. 2, let. b, LPD et les garanties spécifiques au sens de l'art. 16, al. 2, let. c, LPD comprennent au moins les points suivants:

a. l'application des principes de licéité, de bonne foi, de proportionnalité, de transparence, de finalité et d'exactitude;

b. les catégories de données communiquées et de personnes concernées;

c. le type et la finalité de la communication des données personnelles;

d. le cas échéant, le nom des États ou des organismes internationaux auxquels sont destinées les données personnelles, et les conditions applicables à la communication;



- e. les conditions applicables à la conservation, à l'effacement et à la destruction des données personnelles;
- f. les destinataires ou les catégories de destinataires;
- g. les mesures visant à garantir la sécurité des données;
- h. l'obligation d'annoncer les violations de la sécurité des données;
- i. l'obligation pour le destinataire, lorsqu'il est responsable du traitement, d'informer les personnes concernées par le traitement des données;
- j. les droits de la personne concernée, en particulier:
 - 1. le droit d'accès et le droit à la remise ou à la transmission des données personnelles,
 - 2. le droit de s'opposer à la communication des données,
 - 3. le droit de demander la rectification, l'effacement ou la destruction des données,
 - 4. le droit de saisir en justice une autorité indépendante.

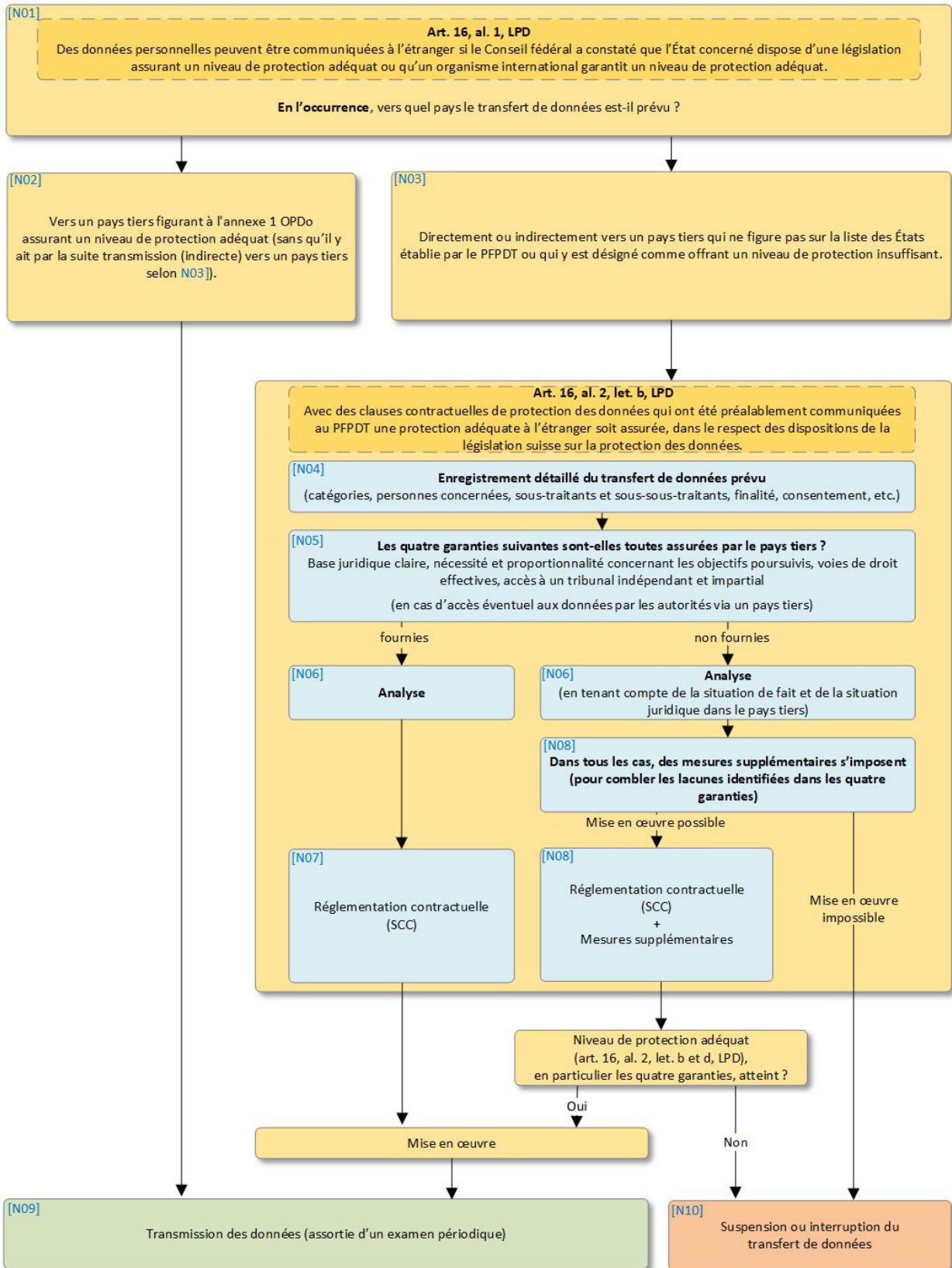
² Le responsable du traitement ou, dans le cas de clauses de protection des données d'un contrat, le sous-traitant prend les mesures adéquates pour s'assurer que le destinataire respecte ces clauses ou les garanties spécifiques.

³ Une fois les clauses de protection des données d'un contrat ou les garanties spécifiques annoncées au PFPDT, le devoir d'information du responsable du traitement est réputé également rempli pour toutes les communications:

- a. qui se fondent sur les mêmes clauses ou garanties, pour autant que les catégories de destinataires, les finalités du traitement et les catégories de données communiquées soient similaires, ou
- b. qui sont effectuées au sein d'une même personne morale ou société ou entre des entreprises appartenant au même groupe.



2. Schéma illustrant le déroulement de la procédure





3. Explications

[N01] Vérification du niveau de protection des données dans le pays tiers

Le responsable de l'exportation des données doit s'assurer qu'un niveau de protection des données adéquat sera garanti lors du traitement des données dans les pays de destination (art. 6 LPD). Si les données sont transférées vers un pays de l'UE ou de l'EEE, on peut considérer que le niveau de protection est adéquat si l'on a la certitude que les données ne seront pas réexportées vers un pays tiers.

Il convient de noter qu'un tiers mandaté pour traiter des données (sous-traitant) qui se trouve dans un pays offrant un niveau de protection des données adéquat peut, suivant les circonstances, être soumis à une loi ou à d'autres exigences d'un pays tiers qui l'oblige à communiquer les données aux autorités d'un pays tiers, et que ces communications peuvent être non transparentes ou non justiciables (voir à ce propos les garanties figurant sous N05). Dans ce cas, il convient de procéder conformément aux indications figurant sous N03 (ex. : serveur situé en Suisse, dans l'UE ou dans l'EEE qui appartient à une entreprise soumise directement ou indirectement à l'ordre juridique d'un État qui n'offre pas un niveau de protection des données adéquat).

[N02] Caractère adéquat (art. 16, al. 1, LPD)

L'État dans lequel les données doivent être exportées figure dans l'annexe 1 de l'OPDo

Si le maître des fichiers transfère des données vers un État qui figure dans l'annexe 1 de l'OPDo en tant qu'État disposant d'un niveau de protection des données adéquat, il est considéré comme étant de bonne foi au sens de l'art. 3, al. 1, CC. Il s'agit toutefois d'une présomption réfutable. Le maître du fichier ne peut pas invoquer sa bonne foi s'il sait par exemple que, dans son cas particulier, le niveau adéquat de protection des données n'est pas garanti dans un pays donné (art. 3, al. 2, CC).

Dans tous les cas, l'exportateur de données reste responsable de l'exportation des données et doit vérifier périodiquement si le niveau de protection est toujours adéquat et s'il n'y a pas d'autres raisons (par ex. sur la base d'indications provenant de la pratique ou des médias) qui s'opposent à un traitement sûr des données personnelles dans le pays de destination considéré.

[N03] Absence de protection adéquate selon la liste des États établie par le PFPDT ou indices selon lesquels aucun transfert de données conforme à la protection des données n'est possible (art. 16, al. 2, let. b et d, LPD)

Si le pays ne figure pas dans l'annexe 1 OPDo en tant qu'État disposant d'un niveau de protection des données adéquat ou si, malgré sa présence dans l'annexe, il existe des indices concrets qu'on ne peut pas considérer le niveau de protection des données comme étant adéquat dans la perspective de l'exportation envisagée, l'exportateur de données doit assurer la protection des données en fournissant les clauses de protection des données d'un contrat entre le responsable du traitement ou le sous-traitant et son cocontractant, préalablement communiquées au PFPDT ou des clauses type de protection des données préalablement approuvées, établies ou reconnues par le PFPDT.



[N04] Enregistrement détaillé du transfert de données

Un enregistrement détaillé du transfert de données par l'exportateur de données, par exemple au moyen d'un répertoire, constitue le fondement pertinent de toute évaluation de l'exportation de données prévue.

Il s'agit notamment d'apporter des réponses aux questions suivantes :

- Les données à exporter ont-elles un caractère personnel ?
- Des personnes seront-elles identifiées ou identifiables ?
- Quelle est la finalité de la communication de données ?
- Quelles sont les catégories de données personnelles qui seront transférées ?
- Y a-t-il d'autres sous-traitants ou sous-sous-traitants ? Dans l'affirmative, se trouvent-ils dans des pays tiers ?
- Les données personnelles seront-elles traitées par des entreprises soumises à des ordres juridiques de pays tiers (par ex. des fournisseurs de cloud américains disposant de serveurs en Suisse/dans l'UE/dans l'EEE) ?
- Les données seront-elles transférées à l'intérieur du pays tiers ou vers un autre pays tiers, ou existe-t-il des indications selon lesquelles ce cas de figure pourrait se produire ?

[N05] Quatre garanties

En ce qui concerne l'accès des autorités du pays tiers aux données (par ex. à des fins de sécurité nationale ou de poursuite pénale) et les droits des personnes concernées, l'exportateur de données doit vérifier si ces accès sont compatibles avec le droit suisse de la protection des données et avec les principes constitutionnels suisses. Il doit procéder lui-même aux clarifications nécessaires sans se fier aux seules déclarations de l'importateur de données. Il peut le faire en consultant la doctrine et la jurisprudence ou en demandant des avis de droit indépendants.

Les garanties ci-après des droits fondamentaux en Suisse doivent exister sous une forme analogue dans le pays tiers, et il convient d'examiner quelles sont les lacunes qui existent dans ce pays :

1. Principe de légalité : règles claires, précises et accessibles (art. 5 et 164 Cst.)

Base juridique suffisamment spécifique et claire concernant les buts, la procédure d'accès aux données par les autorités, les conditions juridiques matérielles de cet accès et les prérogatives des autorités en question.

2. Proportionnalité des prérogatives et des mesures par rapport aux objectifs des réglementations (art. 5, al. 2, Cst. et art. 4, al. 2, LPD)

Les prérogatives des autorités et les mesures qu'elles prennent doivent être appropriées et nécessaires pour atteindre les buts légaux de l'accès des autorités aux données. Elles doivent en outre être raisonnablement exigibles.



3. Toute personne doit disposer de voies de droits effectives (art. 13, al. 2, Cst., dans l'optique de l'application de l'art. 15 LPD, et art. 8 et 13 CEDH)

En Suisse, les personnes concernées doivent disposer de voies de droit effectives, inscrites dans la loi, pour faire valoir leurs droits en matière de protection de la sphère privée et d'autodétermination informationnelle (par ex. droit d'accès, droit de rectification et droit de suppression).

4. Garantie de l'accès au juge et accès à un tribunal indépendant et impartial (art. 29 ss Cst., art. 32 LPD ainsi que l'art. 6 al. 1 CEDH)

Les atteintes à la vie privée et l'autodétermination informationnelle doivent être soumises à un système de contrôle efficace, indépendant et impartial (tribunal ou autre organe indépendant, par ex. une autorité administrative ou un organe parlementaire). Il faut pouvoir contrôler l'approbation (judiciaire) préalable de mesures de surveillance (protection contre l'arbitraire) et le fonctionnement effectif du système de surveillance.

Remarque concernant les États-Unis

S'il existe des indications selon lesquelles des données personnelles seront ou pourraient être traitées directement ou indirectement aux États-Unis, en particulier lors de l'utilisation de services de cloud, le questionnaire figurant en annexe peut être utilisé pour obtenir des précisions [« *Questionnaire de protection des données adressé aux prestataires de services/fournisseurs ayant d'éventuelles relations directes ou indirectes avec les États-Unis (y compris leurs sous-traitants, sous-sous-traitants et autres prestataires de services/fournisseurs)* »].

[N06] Analyse

Une analyse du transfert de données doit être effectuée dans chaque cas, en fonction de l'instrument choisi, par ex. des SCC, et en fonction des conditions juridiques prévalant dans le pays tiers. Lors de l'enregistrement et de l'analyse du transfert de données, l'exportateur de données responsable doit procéder à toutes les clarifications nécessaires (par ex. demander des avis de droit indépendants).

L'examen doit prendre en compte notamment les éléments suivants :

- les prescriptions juridiques en vigueur dans le pays de destination ;
- la pratique des autorités administratives et des autorités judiciaires ;
- la jurisprudence.

[N07] Garanties assurées : SCC

Si les quatre garanties (voir N05) sont assurées, un niveau adéquat de protection des données peut être atteint au moyen de SCC.

Il ne reste alors plus qu'à examiner, dans le cadre de la mise en œuvre des SCC, si d'autres mesures contractuelles de protection (non dirigées contre les accès opérés par l'État) s'imposent. Ces réglementations pourraient par exemple englober les mesures suivantes :



- renforcer les droits des personnes concernées (par ex. le droit d'accès) ;
- prévoir des mesures techniques comme condition du transfert de données ;
- renforcer les prérogatives de l'exportateur de données en obligeant l'importateur de données à se soumettre à des inspections des systèmes de traitement des données et à en rendre compte ;
- prévoir des clauses permettant des procédures rapides de sauvegarde des données en cas de besoin.

[N08] Garanties non fournies : SCC et mesures supplémentaires impératives

Si les garanties mentionnées sous N05 ne sont pas entièrement fournies dans le pays tiers, il convient en tout cas d'examiner au préalable la possibilité de prendre des mesures supplémentaires qui se substitueraient aux garanties manquantes.

Il n'est guère possible de prendre des **mesures contractuelles supplémentaires** (concernant à la fois l'exportateur de données et l'importateur de données), car elles ne peuvent pas lier les autorités de pays tiers et ne peuvent donc pas empêcher l'accès des autorités aux données. Par ailleurs, les réglementations relatives aux dommages et intérêts, la garantie des voies de recours et de l'épuisement de ces dernières pour s'opposer aux injonctions des autorités, ou encore la présentation de rapports sur la transparence, sont des mesures insuffisantes, surtout si les exigences juridiques dans le pays tiers priment ou contrecarrent ces mesures contractuelles.

Les **mesures techniques et organisationnelles supplémentaires** doivent être conçues de telle sorte que les autorités du pays de destination ne puissent pas, dans les faits, accéder aux données personnelles transférées. Dans le cas d'un stockage de données par un prestataire gérant un simple cloud dans un État ne disposant pas d'un niveau de protection adéquat, il serait envisageable d'effectuer par exemple un chiffrement qui serait mis en œuvre selon le principe BYOK (« bring your own key »), doublé du principe BYOE (« bring your own encryption »), de sorte qu'aucune donnée en clair ne soit disponible dans le cloud en question et qu'aucun chiffrement et qu'aucun déchiffrement n'y soient opérés. Toutefois, dans le cas de prestations fournies dans le pays de destination qui vont au-delà du simple stockage de données, l'application de mesures techniques de ce type est ardue.

Si l'examen montre que l'absence d'une ou de plusieurs des quatre garanties mentionnées sous N05 ne peut pas être compensée par des mesures supplémentaires, la procédure selon N10 doit être appliquée.

[N09] Transmission des données

Après avoir mis en œuvre les mesures supplémentaires nécessaires, l'exportateur de données responsable doit vérifier régulièrement si les exigences techniques et juridiques sont respectées. S'il arrive à la conclusion que ce n'est plus le cas, il doit procéder conformément à N10.

[N10] Suspension ou interruption du transfert de données vers l'étranger

Si des mesures supplémentaires ne permettent pas de compenser les lacunes constatées dans le respect des quatre garanties et si, par conséquent, aucune garantie suffisante au sens de



l'art. 6, al. 2, let. a, LPD n'est fournie, le transfert de données vers l'étranger doit être immédiatement suspendu ou interrompu.



Annexe¹

Questionnaire de protection des données adressé aux prestataires de services/fournisseurs ayant d'éventuelles relations directes ou indirectes avec les États-Unis (y compris leurs sous-traitants, sous-sous-traitants et autres prestataires de services/fournisseurs)

Prestataires de services/fournisseurs, y compris tous les sous-traitants et les prestataires de services auxquels il a été fait appel par la suite (également pour les composants logiciels), ci-après « VOUS »

À la lumière de l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-311/18 et en particulier de ses paragraphes 138 à 145, mais pas exclusivement, nous demandons instamment des éclaircissements sur les questions suivantes :

1 Application directe de l'U.S. Code (titre 50, § 1881a) [= FISA 702]

1.1 Est-ce que VOUS, ou toute autre entité américaine concernée (responsable du traitement ou sous-traitant) qui traite des données à caractère personnel qui VOUS sont transmises ou qui a accès à ces données, relevez de l'une des définitions ci-après figurant dans l'U.S. Code [titre 50, § 1881(b)(4)], laquelle pourrait faire en sorte que VOUS ou l'autre/les autres entités soyez directement soumis à l'U.S. Code (titre 50, § 1881a) [= FISA 702] ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question.

1.2 En particulier,

A. Est-ce que VOUS, ou toute autre entité américaine concernée, êtes une entreprise de télécommunications telle que ce terme est défini dans l'U.S. Code (titre 47, § 153) ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

B. Est-ce que VOUS, ou toute autre entité américaine concernée, êtes un fournisseur de services de communications électroniques tel que ce terme est défini dans l'U.S. Code (titre 18, § 2510) ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

C. Est-ce que VOUS, ou toute autre entité américaine concernée, êtes un fournisseur de service informatique à distance tel que ce terme est défini dans l'U.S. Code (titre 18, § 2711) ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

¹ Le présent questionnaire a été adapté et développé pour la Suisse sur la base du questionnaire figurant sur le site www.noyb.eu.



D. Est-ce que VOUS, ou toute autre entité américaine concernée, êtes un autre fournisseur de services de communication qui a accès à des communications filaires ou électroniques, soit lorsque ces communications sont transmises, soit lorsque ces communications sont stockées ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

E. Est-ce que VOUS, ou toute autre entité américaine concernée, êtes un dirigeant, un employé ou un représentant d'une entité entrant dans le champ d'application des let. A, B, C ou D ci-dessus ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

2.1 Êtes-VOUS contrôlé par une société mère américaine ou par un actionnaire américain, ou avez-VOUS un autre lien pertinent avec les États-Unis qui pourrait VOUS soumettre indirectement au droit américain ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

2.2 Dans l'affirmative, êtes-VOUS tenu, en vertu du droit de l'UE, du droit national, du droit des sociétés ou du droit international privé, d'ignorer tout ordre, toute demande et toute directive d'une entité américaine qui vous obligerait à divulguer des données à caractère personnel que VOUS traitez au gouvernement américain en vertu de l'U.S. Code (titre 50, § 1881a) [= FISA 702] ou de l'EO 12.333, et êtes-VOUS effectivement en mesure de bloquer l'accès à ces données ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

VOUS êtes prié d'indiquer les mesures de protection de nature juridique et/ou technique auxquelles VOUS vous référez :

3 Traitement sous le régime de l'EO 12.333



Est-ce que VOUS, ou toute autre entité américaine concernée (responsable du traitement ou sous-traitant) qui traite des données à caractère personnel que nous VOUS avons transmises, coopérez de quelque manière que ce soit avec les autorités américaines qui effectuent la surveillance des communications en vertu de l'EO 12.333, que cette coopération soit obligatoire ou volontaire ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

4 Autres lois applicables

Est-ce que VOUS, ou toute autre entité américaine concernée (responsable du traitement ou sous-traitant) qui traite des données à caractère personnel que nous VOUS avons transmises, êtes soumis à une autre loi qui pourrait être considérée comme affectant la protection des données à caractère personnel au sens du RGPD (article 44) ou du droit suisse ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

Dans l'affirmative, VOUS êtes prié d'indiquer les lois en question :



5 Mesures contre le traitement en masse et sans distinction des données en transit (FISA 702 et EO 12.333)

Comme la cour de justice a elle aussi souligné, dans l'arrêt susmentionné, la nécessité de veiller à ce que les données à caractère personnel en transit ne fassent pas l'objet d'une surveillance de masse, nous vous demandons d'apporter les clarifications suivantes :

A. Avez-VOUS pris les mesures techniques et organisationnelles appropriées (voir article 32 RGPD) pour chaque étape des opérations de traitement afin de rendre impossible le traitement en masse et sans distinction des données à caractère personnel en transit par des autorités ou pour leur compte (par ex. dans le cadre du programme « Upstream » aux États-Unis) ?

Oui Non Nous sommes tenus par la loi de ne pas répondre à cette question

B. Dans l'affirmative, VOUS êtes prié d'indiquer quelles mesures techniques et organisationnelles (y compris le chiffrement) ont été prises pour garantir que ni les données relatives aux contenus ni les métadonnées ne pourront être traitées par des acteurs gouvernementaux hautement développés ayant un accès direct notamment à la dorsale Internet, à des *switches* (commutateurs), à des *hubs* (concentrateurs) et à des câbles :

6 Réponses aux questions ci-dessus

Nous vous demandons de bien vouloir répondre à ces questions dans les plus brefs délais, mais au plus tard dans les cinq jours ouvrables suivant la réception du présent questionnaire.

[Lieu et date]

[Société]

[Signature juridiquement valable]